Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215975

Applications of Zero-Knowledge Proofs for Verifiable Optimization in Local Energy Markets (LEMs)

Zastosowania dowodów wiedzy zerowej do uwierzytelniania obliczeń optymalizacyjnych na lokalnych rynkach energii LEM

Izabela ZOLTOWSKA
Politechnika Warszawska
ORCID: 0000-0002-6563-099X
E-mail: i.zoltowska@elka.pw.edu.pl

Dominika CZERWIŃSKA
Politechnika Warszawska
E-mail: dominika.czerwinska.stud@pw.edu.pl

Abstract

The Local Energy Market (LEM) is a key element in the energy sector's transition toward a decentralized system, enabling the integration of a growing number of small generation sources and energy storage facilities located at end-user locations. By utilizing digital energy trading platforms provided by LEMs, small consumers, producers, and prosumers actively participate in system balancing, which, among others, allows them to increase profits and energy independence. The efficiency of energy exchange in LEM is achieved by means of optimization methods that make use of sensitive participant data, such as energy consumption profiles. Therefore, ensuring privacy while simultaneously ensuring trust in the achieved optimal quantitative and qualitative results is crucial.

The classic technology used in decentralized systems, i.e., blockchain, does not provide adequate scalability when transactions result from solving optimization problems. In this article, we analyze the possibilities of verifying optimization results by the use of cryptographic zero-knowledge proofs (ZKP). We explain how ZKP can support privacy and enable verification of computations without the need of repeating them for every participant. We also refer to existing ZKP implementations on LEM, while highlighting the barriers of high computational costs that prevent direct implementation of complex optimization algorithms within ZKP protocols. ‘

To overcome these barriers, we present an approach integrating ZKP with optimality certificates, which has significant potential to increase the efficiency of

verification of optimization calculations on LEM. This paper aims to initiate a discussion on this new promising method for building trust in LEM balancing systems.

Keywords

smart grids, prosumers, blockchain, market optimization, data privacy, duality

Streszczenie

Lokalny rynek energii (ang. Local Energy Market – LEM) to kluczowy element tranzycji sektora energetycznego w stronę zdecentralizowanego systemu umożliwiającego integrację rosnącej liczby małych źródeł wytwórczych oraz magazynów energii zlokalizowanych u odbiorców końcowych. Poprzez wykorzystanie cyfrowych platform obrotu energią udostępnianych przez LEM-y, drobni odbiorcy, wytwórcy i prosumenci aktywnie uczestniczą w bilansowaniu systemu, co zwiększa m.in. ich zyski oraz niezależność energetyczną. Efektywność procesów wymiany energii na LEM jest osiągana poprzez stosowanie metod optymalizacji, które bazują na wrażliwych danych uczestników, takich jak profile zużycia energii. Kluczową kwestią jest więc zapewnienie prywatności, przy jednoczesnym zapewnieniu zaufania co do osiągniętych, optymalnych wyników ilościowych i wartościowych.

Klasyczna technologia stosowana w systemach zdecentralizowanych, czyli blockchain nie zapewnia odpowiedniej skalowalności, gdy transakcje wynikają z rozwiązania zadania optymalizacji. W tym artykule analizujemy możliwości uwierzytelniania zdecentralizowanych obliczeń optymalizacyjnych poprzez wykorzystania kryptograficznej technologii dowodów wiedzy zerowej (ang. Zero Knowledge Proofs – ZKP). Wyjaśniamy, jak może ona wspierać prywatność i umożliwiać weryfikację poprawności obliczeń, bez konieczności ich bezpośredniego powtarzania, odnosząc się do istniejących implementacji ZKP na LEM.

Wskazujemy na bariery wynikające z wysokich kosztów obliczeniowych, uniemożliwiających realizację złożonych algorytmów optymalizacyjnych bezpośrednio w ramach protokołów ZKP. Przedstawiamy też podejście integrujące ZKP z certyfikatami optymalności, które ma duży potencjał zniwelowania problemów implementacyjnych i zwiększenia efektywności weryfikacji obliczeń optymalizacyjnych na LEM. Artykuł ten ma na celu zainicjowanie dyskusji nad nowymi, bardziej skalowalnymi metodami budowania zaufania w zdecentralizowanych systemach bilansowania LEM.

Słowa kluczowe

smart grids, prosumenci, blockchain, rynkowe mechanizmy optymalizacji, prywatność danych, teoria dualności

Wstęp

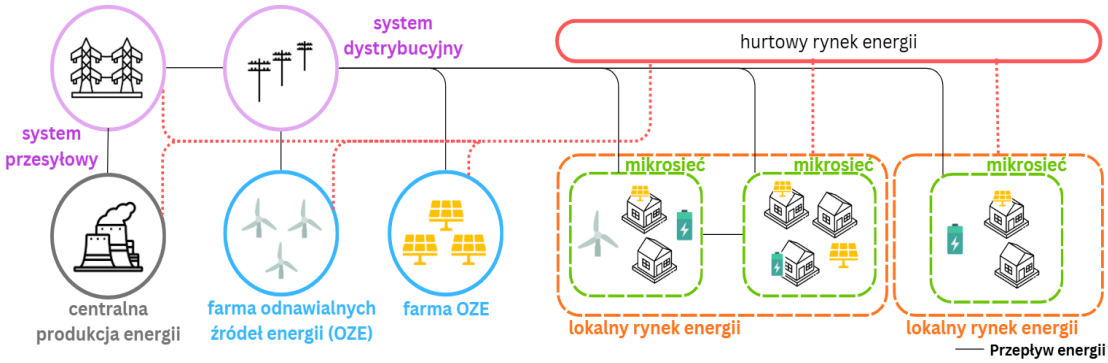
Wraz z rozwojem systemów elektroenergetycznych obserwuje się rosnącą liczbę małych źródeł wytwarzania energii (w tym źródeł odnawialnych) zlokalizowanych u odbiorców. Zgodnie z raportem Unii Europejskiej[1], do 2050 roku połowa Europejczyków ma odpowiadać za połowę generacji ze źródeł odnawialnych. Jest to przyczyną wielu wyzwań i nowych problemów dla operatorów systemów. Konwencjonalne systemy i mechanizmy zostały stworzone z myślą o scentralizowanej produkcji dużej mocy, więc ich architektura utrudnia efektywną integrację rozproszonych zasobów energetycznych (ang. Distributed Energy Resources – DER). W efekcie, przy wzroście udziału DER

[1] Going climate-neutral by 2050 – A strategic long-term vision for a prosperous, modern, competitive and climate-neutral EU economy, Publications Office, 2019, https://data.europa.eu/doi/10.2834/02074 [dostęp: 12.10.2025].

zasadniczo niewidocznych dla operatora systemu, coraz więcej problemów sprawia zapewnienie stabilności pracy systemu i przeprowadzanie procesów bilansowania energii. W odpowiedzi na te problemy narodziła się potrzeba przyjęcia zdecentralizowanego modelu zarządzania energią, który pozwoli w pełni wykorzystać potencjał zasobów rozproszonych. Kluczowym rozwiązaniem stała się koncepcja lokalnych rynków energii (ang. Local Energy Market – LEM), która opiera się na tworzeniu i wykorzystywaniu cyfrowych platform wymiany i obrotu energią zlokalizowaną w bliskim obszarze geograficznym. LEM-y umożliwiają małym graczom rynkowym na aktywne uczestniczenie w bilansowaniu energii na poziomie lokalnym. W ten sposób promują rynkowe podejście do integracji DER, jednocześnie wspierając procesy demokratyzacji energetyki i decentralizacji całego sektora energetycznego, zgodnie z ideami smart grids. Poglądowe umiejscowienie LEM-ów w całościowym systemie elektroenergetycznym przedstawia **Błąd! Nie można odnaleźć źródła odwołania.**.

Kluczowe w koncepcji LEM jest projektowanie mechanizmów dzielenia się energią, określających reguły bilansowania i wyceny, co stanowi podstawę działania platform obrotu. Dąży się do projektowania reguł pozwalających uczestnikom takich rynków na osiąganie korzyści finansowych, ale też będących postrzegane jako proste, a przy tym bezpieczne i sprawiedliwe. To powinno zachęcać uczestników do zaangażowania i aktywnego udziału w LEM. Największa efektywność procesów wymiany energii na LEM jest osiągana poprzez stosowanie metod optymalizacji, które bazują na wrażliwych danych uczestników, takich jak profile zużycia energii. Wyzwaniem jest więc zapewnienie prywatności, przy jednoczesnym zapewnieniu zaufania co do osiągniętych, optymalnych wyników ilościowych i wartościowych. Niniejszy artykuł analizuje możliwości i ograniczenia wykorzystania kryptograficznej technologii dowodów wiedzy zerowej (ang. *Zero Knowledge Proofs* – ZKP) do uwierzytelniania obliczeń optymalizacyjnych i przedstawia koncepcyjne podejście hybrydowe.

Rys. 1. *Umiejscowienie lokalnych rynków energii w systemie elektroenergetycznym.*



Źródło: *opracowanie własne.*

Lokalne rynki energii: mechanizmy bilansowania i wyzwania uwierzytelniania

Koncepcja organizacji obrotu energią na rynkach lokalnych sięga lat 90-tych, przy czym dopiero od ostatnich kilkunastu lat widać duży wzrost zainteresowania w literaturze naukowej, ale też powstawanie rzeczywistych przykładów LEM, często jako pilotażowe efekty licznych projektów europejskich. Do najwcześniejszych, dobrze rozpoznanych i dojrzałych rozwiązań LEM na świecie należą np. Cornwall Local Energy Market, Brooklyn Microgrid (BMG), czy Landau Microgrid Project (LAMP)[2]. Przykłady te stanowią jedynie niewielką część bogatego krajobrazu rynków lokalnych; w rzeczywistości na świecie funkcjonuje i testowanych jest bardzo wiele różnorodnych rozwiązań. Na poziomie Unii Europejskiej dalszy ich rozwój aktywnie wspiera inicjatywa Citizen Energy Advisory Hub (CEAH)[3], która zrzesza społeczności energetyczne ułatwiając im organizację i wymianę doświadczeń. Społeczności takie stanowią pierwszy krok dla formalizowania LEM. W Polsce pierwsza obywatelska społeczność energetyczna MES-TOWN Łódź zawiązała się stosunkowo późno, bo dopiero w kwietniu 2025 roku. Obserwując doświadczenia europejskie, można spodziewać się jednak, że zapoczątkuje to nowy trend.

Ta żywotność tematu w badaniach naukowych i praktyce sprawia, że istnieje mnogość mechanizmów, wspierających różnorakie cele funkcjonowania lokalnych rynków — od optymalizacji kosztów, przez poprawę jakości energii, oferowanie usług operatorom systemów przesyłowych aż po osiągnięcie bezpieczeństwa i niezależności energetycznej. W każdym przypadku centralnym zadaniem LEM jest umożliwienie odbiorcom, wytwórcom, magazynom energii (w tym pojazdom elektrycznym EVs) i prosumentom komunikacji potrzeb oraz możliwości wymieniania się między sobą lokalnie wyprodukowaną energią elektryczną, oraz wspomaganie określania planów zużycia energii – tzw. bilansowania oraz ich rozliczania.

W odniesieniu do LEM można mówić o dwóch podstawowych topologiach rynku, jak też o dwóch podstawowych sposobach bilansowania rynku. Rozwiązania zcentralizowane, zbudowane wokół centralnego podmiotu odpowiedzialnego za zarządzanie rynkiem lokalnym można uznać za najpowszechniejszą topologię spotykaną w literaturze[4]. Taki sposób organizacji LEM ułatwia koordynację z rynkami zewnętrznymi (rynkami hurtowymi, bilansującym, usług systemowych). Z kolei zdecentralizowane topologie rynkowe, skoncentrowane głównie na kwestiach prywatności i preferencji konsumentów zakładają demokratyzację i niezależność podejmowania decyzji nie wymagających zatwierdzania, czy koordynowania przez podmiot pośredniczący. W obu tych podejściach można spotkać się ze scentralizowanymi i zdecentralizowanymi mechanizmami bilansowania, co często prowadzi do tzw. rozwiązań hybrydowych (por. Rys. 2).

Mechanizmy scentralizowane polegają na rozwiązaniu problemu optymalizacyjnego określającego, które podmioty uczestniczą w wymianie

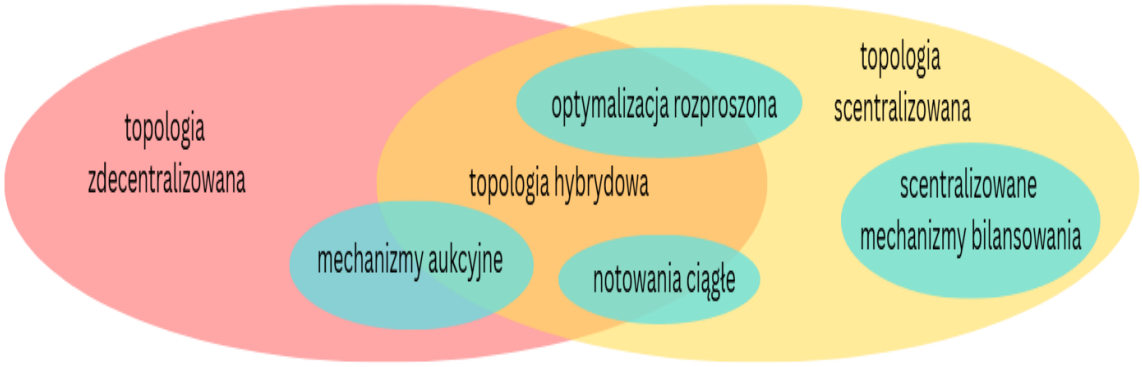
[2] S. Bjarghov i in., Developments and Challenges in Local Electricity Markets: A Comprehensive Review, “IEEE Access” 2021, 9, s. 58910–58943, https://doi.org/10.1109/ACCESS.2021.3071830.

[3] https://citizens-energy.ec.europa.eu/ [dostęp 25.10.2025].

[4] M. Khorasany i in., Market framework for local energy trading: a review of potential designs and market clearing approaches, “IET Generation, Transmission & Distribution” 2018, no. 12(22), s. 5899–5908, https://doi.org/10.1049/IET-GTD.2018.5309.

energii w danych jednostkach czasu, najczęściej jako kryterium przyjmując minimalizację sumarycznych kosztów. Natomiast na rynkach ze zdecentralizowanym bilansowaniem i rozliczeniami, transakcje są wykonywane w sposób wielostronny między podmiotami (tzw. agentami) w systemie, czyli są organizowane na zasadzie handlu P2P (peer-to-peer). Wszyscy producenci energii, prosumenci i aktywni odbiorcy dzielą się informacjami za pośrednictwem platformy transakcyjnej opartej na dynamicznie zmieniających się preferencjach.

Rys. 2. *Topologie LEM oraz rodzaje mechanizmów bilansowania.*



Źródło: *opracowanie własne na podst. S. Bjarghov i in., op.cit. s. 58910.*

Osiągnięcie optymalności na rynku stosującym mechanizmy zdecentralizowane jest trudne, jednak jak pokazano w literaturze, jest możliwe przy założeniu istnienia węzła nadzorującego z dostępem do funkcji użyteczności uczestników rynku. Takie założenie spełniają mechanizmy aukcyjne, które podobnie jak w przypadku mechanizmów scentralizowanych, wykorzystują metody optymalizacji do wyznaczenia rozstrzygnięć – szczególnie gdy mowa o aukcjach obrotu energią, wymagających stosowania bardziej złożonych postaci ofert. Wprowadzenie węzła zbierającego i przekazującego informacje uczestnikom rynku poprawia efektywność, ale może osłabiać zaufanie, poczucie bezpieczeństwa i prywatności danych. Kwestie te są jednak z reguły pomijane przy projektowaniu mechanizmów bilansowania LEM, a główna uwaga poświęcona jest modelowaniu i optymalizacji.

W efekcie, wiele dotychczasowych modeli bilansowania LEM zakłada istnienie zaufanej jednostki centralnej. Takie podejście wiąże się jednak z ryzykiem manipulacji wynikami optymalizacji przez jednostkę centralną, do tego może budzić wątpliwości, gdy poprawa sumarycznej efektywności jest osiągana kosztem pojedynczych uczestników. Przy tym, nie jest proste zweryfikowanie optymalności wyników bez naruszenia prywatności danych. Zwróćmy uwagę, że optymalizacja jest możliwa dzięki dostępowi do informacji prywatnych, które w zależności od przyjętego mechanizmu mogą nawet odnosić się bezpośrednio do danych o profilach zużycia i produkcji energii poszczególnych użytkowników. Weryfikacja poprawności obliczeń przez innych uczestników wymagałaby zatem dostępu do danych pozostałych agentów, co byłoby nieakceptowalne z punktu widzenia prywatności. Publiczne ujawnienie takich informacji – jak np. liczba domowników czy godziny przebywania poza domem – mogłoby prowadzić do realnych zagrożeń bezpieczeństwa.

Z tego powodu w rozwiązaniach dotyczących lokalnych rynków energii coraz częściej wykorzystuje się technologie zapewniające bezpieczeństwo i integralność danych, takie jak blockchain[5]. Blockchain jest rozproszoną strukturą danych – wspólną, współdzieloną bazą transakcji, która przechowuje w sposób niezmienny i uporządkowany chronologicznie rekordy zdarzeń. Każdy blok zawiera zestaw transakcji, jest opatrzony znacznikiem czasu oraz kryptograficznie połączony z blokiem poprzednim, tworząc łańcuch bloków (blockchain). Głównym celem tej technologii jest eliminacja potrzeby zaufanych pośredników poprzez zastąpienie ich rozproszoną siecią, w której każdy uczestnik posiada własną kopię rejestru transakcji. Takie rozwiązanie zapewnia odporność systemu na manipulacje i awarie, ale jednocześnie zwiększa obciążenie obliczeniowe. W klasycznym modelu każdy węzeł jest zobowiązany do samodzielnej weryfikacji wszystkich transakcji zawartych w blokach, co znacząco ogranicza skalowalność i wydajność całej sieci.

Wraz ze wzrostem popularności technologii blockchain pojawiły się zatem koncepcje umożliwiające zwiększenie jej skalowalności. Jednym z podejść jest przeniesienie części obliczeń poza główny łańcuch bloków (off-chain computation) tak, aby procesy wymagające dużych zasobów – takie jak weryfikacja lub agregacja dużej liczby transakcji – mogły być realizowane poza blockchainem, a do rejestru trafiał jedynie skrócony i zweryfikowany wynik obliczeń. Aby było to możliwe, konieczne jest zastosowanie mechanizmów umożliwiających weryfikację poprawności obliczeń bez konieczności ich bezpośredniego powtarzania. Jednym z najbardziej obiecujących rozwiązań w tym zakresie są dowody wiedzy zerowej (ang. Zero Knowledge Proofs – ZKP). Technologia ZKP pozwala na udowodnienie poprawności obliczeń przy zachowaniu pełnej poufności danych wejściowych oraz na bezpieczne wprowadzanie danych zewnętrznych (np. prognoz pogodowych) do łańcucha bloków.

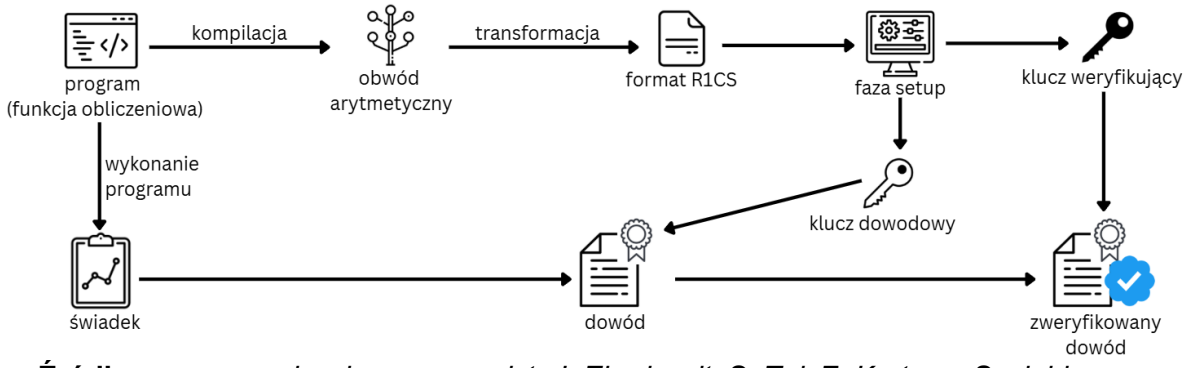
Dowody wiedzy zerowej (ang. Zero Knowledge Proofs – ZKP)

Sposobem ochrony prywatności danych w systemach zdecentralizowanych są dowody wiedzy zerowej (ZKP). Technika ta polega na przedstawieniu dowodu (ang. proof) przez stronę udowadniającą (ang. Prover), który ma przekonać stronę weryfikującą (ang. Verifier), że określone twierdzenie jest prawdziwe, bez ujawniania żadnych informacji, które mogłyby zdradzić, dlaczego to twierdzenie jest prawdziwe. Dowód ten nazywany jest „zerowej wiedzy”, ponieważ osoba weryfikująca nie uzyskuje innej wiedzy poza faktem poprawności twierdzenia. Ważnym elementem koncepcji ZKP jest wykorzystanie pomocniczych tajnych informacji, znanych tylko stronie udowadniającej, nazywanych świadkiem (ang. witness). W typowej sytuacji, gdy strona udowadniająca przeprowadza pewne obliczenia, to twierdzenie sprowadza się do postulowania ich poprawności, a świadkiem są wygenerowane dane wejściowe i odpowiadające im wyniki. Wystarczy wtedy wykazać, że strona udowadniająca zna świadka, czyli rozwiązanie określonego problemu, ale bez ujawniania jego wartości.

[5] M. Andoni i in., Blockchain technology in the energy sector: A systematic review of challenges and opportunities, “Renewable and Sustainable Energy Reviews” 2019, no. 100, s. 143–174, https://doi.org/10.1016/j.rser.2018.10.014.

Forma dowodu w kontekście ZKP ma ściśle określone znaczenie kryptograficzne, jest to matematyczne sformułowanie problemu odpowiadające pełnym obliczeniom w taki sposób, aby umożliwić weryfikację na wygenerowanym zestawie danych (świadku). Sposób generowania i weryfikacji dowodu został przedstawiony na Rys. 3.

Rys. 3. *Schemat tworzenia dowodu w technologii ZKP.*



Źródło: *opracowanie własne na podst. J. Eberhardt, S. Tai, ZoKrates – Scalable Privacy-Preserving Off-Chain Computations, IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) 2018, s. 1084–1091, https://doi.org/10.1109/ Cybermatics_2018.2018.00199.*

Obliczenia są przekształcane w tzw. obwód arytmetyczny (ang. Arithmetic Circuit), którego struktura określa relacje pomiędzy zmiennymi wejściowymi, pośrednimi i wyjściowymi. W odróżnieniu od klasycznej architektury von Neumanna, w której instrukcje są wykonywane sekwencyjnie przez procesor, obwód arytmetyczny opisuje wszystkie operacje jako statyczną sieć połączeń między bramkami dodawania i mnożenia. Oznacza to, że przepływ danych i zależności między operacjami muszą być określone z góry. Taka reprezentacja wymaga pełnego rozwinięcia logiki programu przed rozpoczęciem obliczeń, co prowadzi do dużych rozmiarów obwodów dla bardziej złożonych algorytmów. Obwód tworzony jest automatycznie za pomocą specjalnych kompilatorów lub frameworków (np. Circom, ZoKrates), które tłumaczą kod programu służącego do obliczeń na reprezentację arytmetyczną wykorzystywaną w protokołach ZKP. Następnie obwód arytmetyczny jest odwzorowywany jest w formie Rank-1 Constraint System (R1CS) – matematycznego systemu ograniczeń, który reprezentuje logikę programu jako zbiór równań kwadratowych. Każde równanie w R1CS odpowiada relacji między zmiennymi w obwodzie, a cały system stanowi algebraiczną reprezentację programu możliwą do użycia w konstrukcjach kryptograficznych.

Protokół ZKP gwarantuje, że nie da się przekonująco udowodnić znajomości świadka, bez przeprowadzenia poprawnych obliczeń. Istnieje wiele protokołów implementacji koncepcji ZKP. Różnią się one sposobem zapisu dowodu oraz regułami wymiany informacji między zainteresowanymi stronami. Dowód jest zazwyczaj znacznie krótszy niż pełny zapis potwierdzanych obliczeń, a jego rozmiar (ang. *proof size*) – czyli liczba bitów potrzebna do jego zapisu, stanowi kluczowy parametr efektywności wybranego protokołu ZKP. W zależności od konstrukcji protokołu, dowody mogą mieć charakter interaktywny, gdzie osoba udowadniająca i weryfikująca wymieniają serię

komunikatów, lub nieinteraktywny, w którym cały proces sprowadza się do jednorazowego przekazania gotowego dowodu. Tradycyjne protokoły ZKP zapewniają wysoki poziom bezpieczeństwa i prywatności, jednak w praktyce ich zastosowanie w złożonych obliczeniach – takich jak optymalizacja w lokalnych rynkach energii – może być kosztowne obliczeniowo i czasochłonne, gdyż rozmiar dowodu oraz czas jego weryfikacji rosną wraz ze złożonością obliczeń. Do tego, mają zwykle charakter interaktywny, więc potwierdzenie dowodu przez wielu uczestników weryfikujących wymaga jego oddzielnego przesłania i przetworzenia przez każdego z nich.

W odpowiedzi na te ograniczenia opracowano zkSNARK (ang. Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) – szczególny sposób implementacji ZKP realizujący mechanizm weryfikowalnych obliczeń (ang. Verifiable Computation). W podejściu tym generowany jest krótki (ang. succint) względem złożoności obliczeń dowód kryptograficzny potwierdzający, że obliczenia zostały wykonane poprawnie, bez potrzeby ich ponownego uruchamiania. Potwierdzenie takiego dowodu wymaga minimalnych zasobów obliczeniowych, bez potrzeby dalszej komunikacji między stronami (ang. non-interactive), gdyż zkSNARK zapewnia publiczną weryfikowalność.

W rodzinie protokołów zkSNARK proces generowania dowodu rozpoczyna się od fazy inicjalizacji (ang. setup). W jej trakcie tworzony jest zestaw kluczy kryptograficznych:

- klucz dowodowy (ang. proving key) – wykorzystywany przez stronę udowadniającą do generowania dowodu,
- klucz weryfikujący (ang. verification key) – używany przez stronę sprawdzającą do potwierdzenia poprawności wygenerowanego dowodu.

Następnie strona udowadniająca uruchamia obliczenia w celu uzyskania rozwiązania –świadka, czyli konkretnych wartości wynikowych i pośrednich spełniających wszystkie równania R1CS dla wygenerowanych zmiennych wejściowych. Korzystając z wartości świadka oraz klucza dowodowego, strona udowadniająca generuje dowód kryptograficzny. Strona weryfikująca może publicznie zweryfikować dowód przy użyciu klucza weryfikującego. Jeśli dowód jest poprawny, strona weryfikująca uzyskuje pewność, że obliczenia zostały wykonane zgodnie z założeniami programu – bez konieczności ich powtarzania i bez ujawniania danych wejściowych.

Protokoły zkSNARK znajdują zastosowanie wszędzie tam, gdzie potrzebne jest potwierdzenie poprawności obliczeń bez ujawniania danych, np. w bezpiecznych systemach płatności, uwierzytelnianiu użytkowników oraz w aplikacjach zapewniających prywatność transakcji. Technika ta budzi też rosnące zainteresowanie w kontekście bezpieczeństwa i ochrony prywatności w LEM.

Jednym z praktycznych zastosowań tej koncepcji jest realizacja procesu bilansowania wzajemnych zobowiązań i należności energetycznych poza łańcuchem bloków (off-chain) przez dedykowaną jednostkę obliczeniową[6]. Jednostka ta wyznacza bilans energii dla uczestników LEM, a następnie przekazuje na blockchain wynik wraz z dowodem wiedzy zerowej potwierdzającym poprawność przeprowadzonych obliczeń. Dzięki temu prywatne dane dotyczące zużycia i produkcji energii pozostają nieujawnione,

[6] J. Eberhardt i in., Privacy-Preserving Netting in Local Energy Grids, 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2020, DOI:10.1109/ICBC48266.2020.9169440.

a jednocześnie integralność i poprawność obliczeń mogą być publicznie zweryfikowane przez wszystkie strony systemu. Rozwiązanie to jednak ogranicza się do weryfikacji prostego bilansu energii, a nie do weryfikacji rozwiązania zadania optymalizacyjnego.

Innym przykładem jest system[7], w którym właściciele pojazdów elektrycznych oraz uczestnicy LEM współpracują w celu zaspokojenia zapotrzebowania energetycznego pojazdów w modelu P2P, korzystając z wirtualnych płatności. W zaproponowanym rozwiązaniu zastosowano ZKP w celu zapewnienia bezpiecznych i anonimowych płatności podczas rozliczania transakcji w zdecentralizowanym środowisku, w którym brak jest zaufanego pośrednika finansowego. Mechanizm ZKP umożliwia użytkownikowi udowodnienie prawa własności cyfrowych monet bez ujawniania ich numerów seryjnych ani jakichkolwiek innych danych identyfikujących, co gwarantuje anonimowość użytkowników, integralność transakcji oraz odporność na podwójne wydatkowanie środków w procesie handlu energią pomiędzy uczestnikami rynku. Ciekawe zastosowanie ZKP dotyczy umożliwienia weryfikacji poprawności obliczeń i rozliczeń dokonywanych przez inteligentne liczniki (smart meters) bez ujawniania szczegółowych danych[8]. ZKP pozwala dostawcy energii sprawdzić prawidłowość naliczonych zagregowanych opłat na podstawie lokalnych odczytów licznika, jednocześnie chroniąc prywatność użytkownika poprzez ukrycie jego indywidualnych profili zużycia. Dzięki temu metoda zapewnia zaufanie i rozliczalność w procesie pomiaru i fakturowania energii, bez potrzeby ujawniania wrażliwych danych profilu godzinowej konsumpcji użytkownika.

W innym badaniu skoncentrowano się na weryfikowalności obliczeń optymalizacyjnych w LEM-ach implementując ZKP w postaci zkSNARK dla algorytmu Simplex[9]. Pokazano, że jest to wykonalne, jednak zupełnie niemożliwe w praktycznych zastosowaniach LEM ze względu na ogromną złożoność obliczeniową. Procedury optymalizacyjne, odwzorowane w postaci obwodów arytmetycznych, muszą bowiem realizować pełną, z góry określoną liczbę iteracji – niezależnie od tego, czy rozwiązanie zostało osiągnięte wcześniej. Wyniki implementacji wykazały, że czas kompilacji, generowania świadków oraz liczba ograniczeń R1CS rosną wykładniczo wraz ze wzrostem liczby zmiennych i ograniczeń w zadaniu optymalizacyjnym. Dla przykładowego problemu z 10 zmiennymi decyzyjnymi i 10 ograniczeniami liczba równań w systemie R1CS osiągnęła rząd wielkości 10^7, co oznacza, że tyle równań algebraicznych musi zostać utworzonych w celu wygenerowania pojedynczego dowodu zkSNARK. Typowe rozmiary problemów LEM są o kilka rzędów większe.

Integracja certyfikatów optymalności z ZKP

Interesującą alternatywą wykorzystania ZKP do uwierzytelniania zadań optymalizacji jest oparcie się na tzw. certyfikacie optymalności, który bezpośrednio korzysta z teorii dualności, stanowiącej matematyczną

[7] E. M. Radi i in., Privacy-Preserving Electric Vehicle Charging for Peer-to-Peer Energy Trading Ecosystems, IEEE International Conference on Communications (ICC), Shanghai, Chinaradi 2019, DOI: 10.1109/ICC.2019.8761788.

[8] C.D. Pop i in., Blockchain and Demand Response: Zero-Knowledge Proofs for Energy Transactions Privacy, Sensors, 2020, no. 20(19), s. 5678, DOI: https://doi.org/10.3390/s20195678.

[9] A. Zeiselmair i in., Analysis and Application of Verifiable Computation Techniques in Blockchain Systems for the Energy Sector, “Front Blockchain” 2021, no. 4, doi:10.3389/fbloc.2021.725322.

charakterystykę warunków optymalności dla zadań programowania liniowego. Zgodnie z teorią dualności, możliwa jest weryfikacja optymalności rozwiązania zadania programowania liniowego poprzez analizę relacji między rozwiązaniem zadania prymalnym i dualnego. Zadanie prymalne można zapisać jako:

$$\max(\boldsymbol{c}^T\boldsymbol{x})$$
$$\boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{b}$$
$$\boldsymbol{x} \geq 0$$

a jego odpowiadającą postać dualną jako:

$$\min(\boldsymbol{b}^T\boldsymbol{y})$$
$$\boldsymbol{A}^T\boldsymbol{y} \geq \boldsymbol{c}$$
$$\boldsymbol{y} \geq 0$$

Gdzie (x, y) oznaczą zmienne, odpowiednio zadania prymalnego i dualnego. Zgodnie z twierdzeniem o optymalności rozwiązania, rozwiązania x* i y* są optymalne wtedy i tylko wtedy gdy spełniają warunek:

$$\boldsymbol{c}^T \cdot \boldsymbol{x}^* = \boldsymbol{b}^T \cdot \boldsymbol{y}^*. \qquad \text{(Tw1)}$$

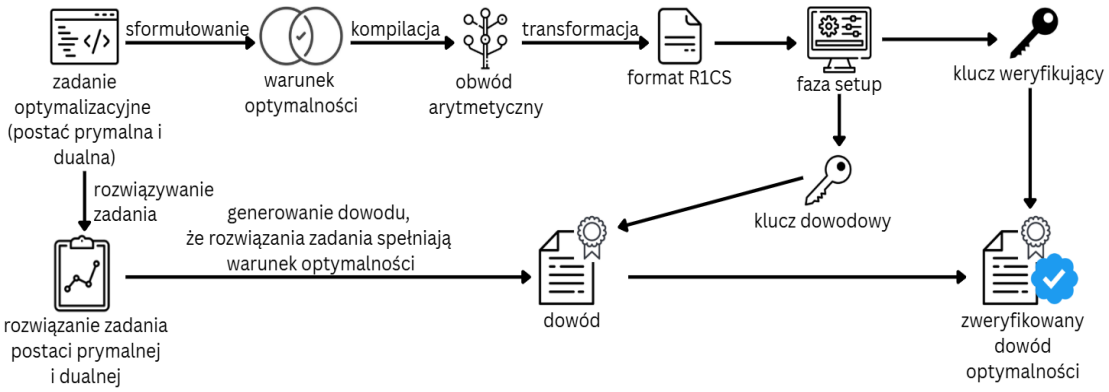
Ta zależność, nazywana certyfikatem optymalności oferuje alternatywną możliwość do sprawdzenia czy rozwiązanie jest poprawne. To znaczy, chcąc sprawdzić czy dane rozwiązanie jest optymalne można albo prześledzić krok po kroku działanie algorytmu rozwiązującego zadanie optymalizacyjne, albo sprawdzić czy jest spełniony warunek Twierdzenia Tw1. Oba podejścia prowadzą do tej samej konkluzji: potwierdzenia lub odrzucenia optymalności. Różnią się jednak nakładem obliczeniowym i stopniem złożoności weryfikacji.

Należy jednak zauważyć, że sam certyfikat optymalności nie rozwiązuje problemu prywatności danych. Aby sprawdzić warunek (Tw1), konieczna jest znajomość wektorów (c i b), które zazwyczaj zawierają poufne informacje o konkretnym zadaniu optymalizacyjnym. Proponowanym rozwiązaniem tego problemu jest integracja ZKP z certyfikatem optymalności. W takim podejściu ZKP zapewnia ochronę poufnych danych, natomiast certyfikat optymalności eliminuje konieczność implementacji całego solvera w formacie R1CS. Taka realizacja jest możliwa zgodnie z następującym schematem[10] (Rys. 4): problem optymalizacyjny należy sformułować oraz rozwiązać w postaci zadania prymalnego i dualnego. Należy też zapisać warunek optymalności (Tw1) w formacie R1CS, co jest stosunkowo proste ponieważ wyrażenie to nie wymaga stosowania pętli czy złożonych operacji arytmetycznych.

Dysponując rozwiązaniami (x*, y*) oraz certyfikatem optymalności zapisanym w formacie R1CS możliwe jest wygenerowanie dowodu ZKP w tradycyjny sposób, czyli chroniąc prywatność wektorów (b i c) z warunku optymalności. Ostatecznie strona udowadniająca udowadnia: „Rozwiązanie zadania to x*, y*, a oto dowód, że te rozwiązania są optymalne dla danych zadania”, podczas gdy w tradycyjnej implementacji ZKP udowadniano: „Rozwiązanie zadania to x*, y*, a oto dowód, że w celu uzyskania rozwiązania wykonałem wszystkie kroki solvera dla danych zadania”.

[10] S. Angel i in., Efficient Representation of Numerical Optimization Problems for SNARKs. Proc 31st USENIX Secur Symp Secur 2022. Published online 2022:4273-4290.

Rys. 4. *Schemat tworzenia dowodu w podejściu integrującym ZKP z certyfikatem dualności.*



Źródło: *opracowanie własne na podst. S. Angel i in., Efficient Representation of Numerical Optimization Problems for SNARKs, Proceedings of the 31st USENIX Security Symposium, Security 2022, s. 4273–4290.*

Takie podejście stanowi obiecujący sposób zastosowania ZKP w zadaniach optymalizacyjnych dla systemów LEM, które często są formułowane w postaci zadań programowania liniowego – a jest to warunek konieczny dla stosowania certyfikatu optymalności.

Zakończenie

Transformacja energetyczna, napędzana przez wzrost udziału DER i rozwój lokalnych rynków energii (LEM), stawia przed mechanizmami bilansowania kluczowe wyzwanie: jak zapewnić wiarygodność procesu optymalizacji przy jednoczesnym zachowaniu pełnej poufności wrażliwych danych uczestników. Tradycyjne podejście wymaga od graczy rynkowych pełnego zaufania do jednostki centralnej (np. operatora rynku), co nie jest zgodne z ideami demokratyzacji i decentralizacji energetyki, będącymi siłą napędową LEM. Jak wykazaliśmy w artykule, zastosowanie dowodów wiedzy zerowej (ZKP) do uwierzytelniania złożonych obliczeń optymalizacyjnych jest technicznie obiecujące, lecz napotyka na poważne bariery związane z wysokimi kosztami obliczeniowymi i brakiem skalowalności. W odpowiedzi na te wyzwania, niniejsza analiza wskazała na hybrydowe podejście, polegające na integracji ZKP z certyfikatami optymalności, czyli wykorzystaniem rozwiązań zadania prymalnego i dualnego. Podejście takie pozwala na rozdzielenie kosztownego procesu optymalizacji (rozwiązywanego przez zewnętrzny solver) od efektywnej weryfikacji certyfikatu w ramach protokołu ZKP co umożliwia bezpieczne i skalowalne uwierzytelnienie obliczeń optymalizacyjnych, przy zachowaniu poufności danych wejściowych. Ten artykuł zarysowuje kierunek dalszych badań nad nowymi, bardziej skalowalnymi metodami budowania zaufania w zdecentralizowanych mechanizmach bilansowania LEM.

Bibliografia

Alqahtani, E., Mustafa, M. A., Privacy-Preserving Local Energy Markets: A Systematic Literature Review, “SSRN Electronic Journal” 2023, https://doi.org/10.2139/ssrn.4483407.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A., Blockchain technology in the energy sector: A systematic review of challenges and opportunities, “Renewable and Sustainable Energy Reviews” 2019, no. 100, https://doi.org/10.1016/j.rser.2018.10.014.

Angel, S., Blumberg, A. J., Ioannidis, E., Woods, J., Efficient Representation of Numerical Optimization Problems for SNARKs, “Proceedings of the 31st USENIX Security Symposium, Security 2022.

Bjarghov, S., Loschenbrand, M., Ibn Saif, A. U. N., Alonso Pedrero, R., Pfeiffer, C., Khadem, S. K., Rabelhofer, M., Revheim, F., Farahmand, H., Developments and Challenges in Local Electricity Markets: A Comprehensive Review, “IEEE Access” 2021, no. 9, https://doi.org/10.1109/ACCESS.2021.3071830.

Eberhardt, J., Tai, S., ZoKrates – Scalable Privacy-Preserving Off-Chain Computations, “IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) 2018, https://doi.org/10.1109/Cybermatics_2018.2018.00199.

Khorasany, M., Mishra, Y., Ledwich, G., Market framework for local energy trading: a review of potential designs and market clearing approaches, “IET Generation, Transmission & Distribution” 2018, no. 12(22), https://doi.org/10.1049/IET-GTD.2018.5309.

Pop, C.D., Antal, M., Cioara, T., Anghel, I., Salomie, I., Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy, “Sensors” 2020, no. 20(19), https://doi.org/10.3390/s20195678.

Radi, E. M., Lasla, N., Bakiras, S., Mahmoud, M., Privacy-preserving electric vehicle charging for peer-to-peer energy trading ecosystems, Proceedings of the 2019 IEEE International Conference on Communications (ICC), https://doi.org/10.1109/ICC.2019.8761788.

Zeiselmair, A., Steinkopf, B., Gallersdörfer, U., Bogensperger, A., Matthes, F., Analysis and application of verifiable computation techniques in blockchain systems for the energy sector, “Frontiers in Blockchain” 2021, no. 4, https://doi.org/10.3389/fbloc.2021.725322.

Zhou, L., Diro, A., Saini, A., Kaisar, S., Hiep, P.C., Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities, “Journal of Information Security and Applications” 2024, no. 80, https://doi.org/10.1016/j.jisa.2023.103678.