

Blockchain

ODPORNE ŹRÓDŁO PRAWDY

Blockchain explained

Seria „**Blockchain Explained**” to łatwy do zrozumienia przewodnik, który obejmuje podstawy technologii blockchain i jej zastosowania. Omawia korzyści i wyzwania związane z wykorzystaniem technologii blockchain, w tym jego zastosowanie w sektorze publicznym na przykładzie EBSI. Seria porusza również kwestie technologicznych komponentów oraz przypadków użycia EBSI.



Pojęcie rejestru jest tak stare jak pismo

Staliśmy się bardziej zaawansowani dzięki rejestrom i księgom scentralizowanym.

Utworzenie rejestrów państwowych było ważnym krokiem naprzód w odróżnianiu fałszywych informacji od prawdziwych.

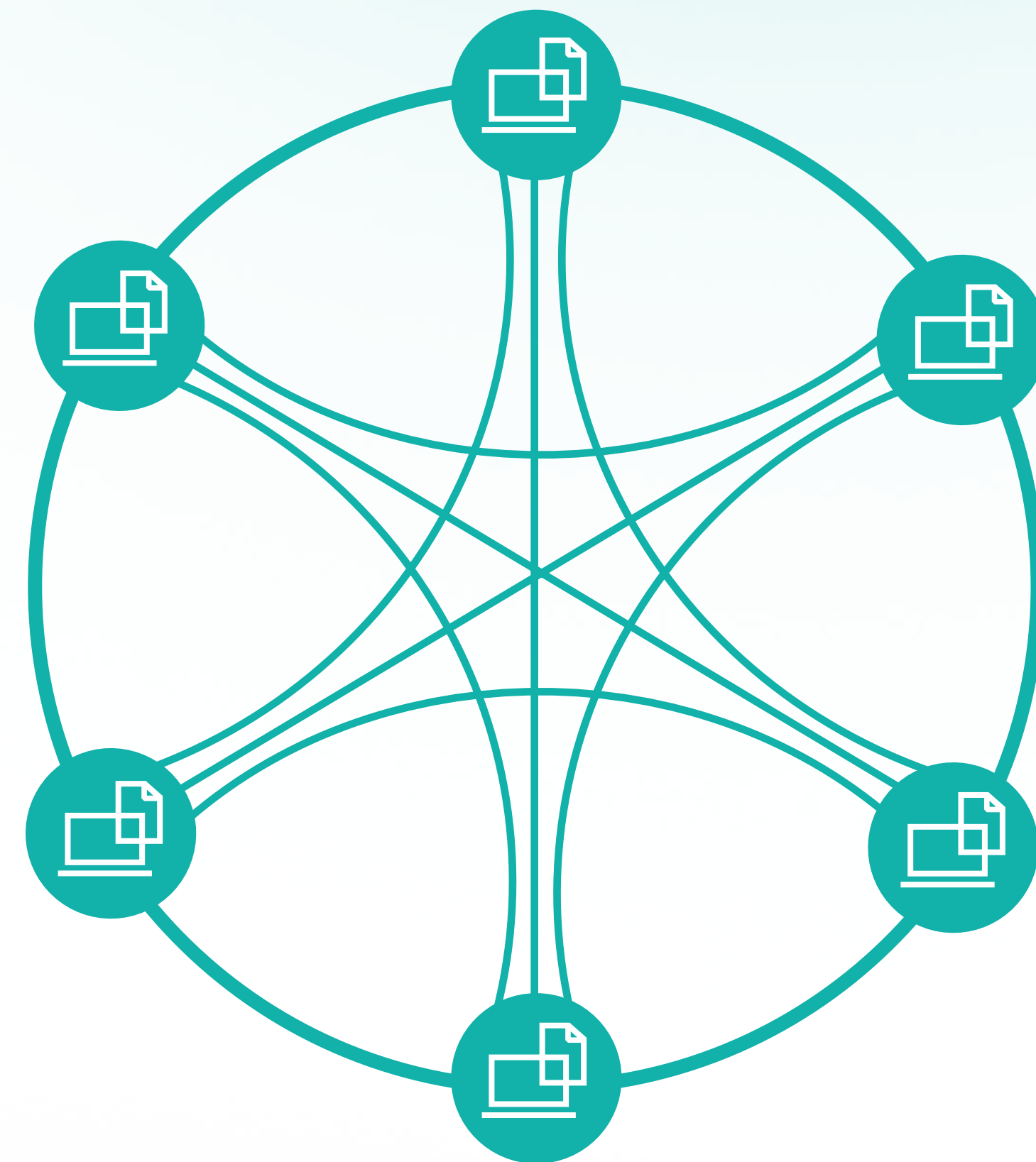
Czym jest blockchain?

Blockchain to po prostu zdecentralizowany / rozproszony rejestr.

REJESTR (ang. *LEDGER*) to dobrze znane pojęcie w biznesie, oznaczające zapisy służące do prowadzenia jednoznacznego rejestru transakcji.

REJESTRY wykorzystywane są do zapisu niemal każdego rodzaju transakcji – na przykład statusu dokumentu.

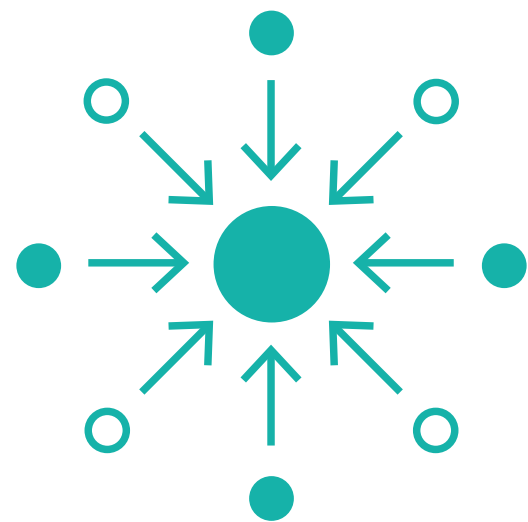
REJESTR ROZPROSZONY (ang. *DISTRIBUTED LEDGER*) tu wpisy przechowywane są w wielu węzłach sieci, zamiast w jednym miejscu, co czyni je odpornymi na manipulacje („tamper-resistant”).



To zupełnie nowe podejście... ...do zarządzania danymi:

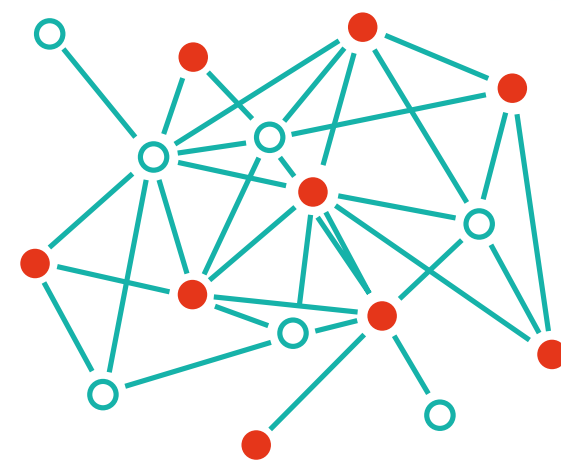
Sieć 1.0:

Podejście scentralizowane



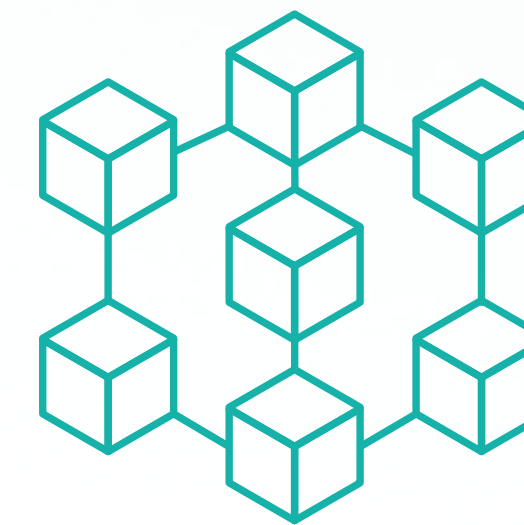
Sieć 2.0:

Podejście federacyjne



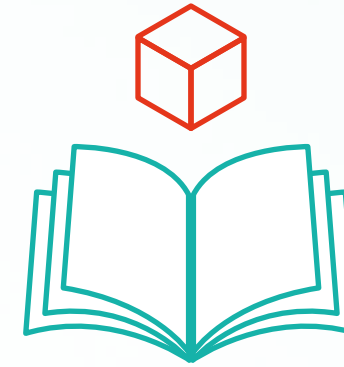
Sieć 3.0:

Podejście rozproszone



Jak działa blockchain?

Objaśnienie przez metaforę:



Wyobraź sobie każdy blok jako **stronę w rejestrze** lub folder w szafie akt.
Tak jak one, blockchain przechowuje różne informacje – transakcje finansowe,
umowy oraz inne dane.

Jednak w przeciwieństwie do nich, blockchain jest **rozproszony między wieloma komputerami**,
co czyni go bardzo bezpiecznym i odpornym na naruszenia i manipulacje.



Blockchain to lista połączona – bloki danych są kryptograficznie powiązane, tworząc łańcuch

1.

Każdy blok zawiera wynik funkcji skrótu (hash) poprzedniego bloku, co zapewnia integralność danych.

2.

Nowe bloki zawierają dane, transakcje i odnośniki do poprzednich bloków (tworzą łańcuch).

3.

Każdy blok zawiera wynik funkcji skrótu utworzony z danych zawartych w bloku.

4.

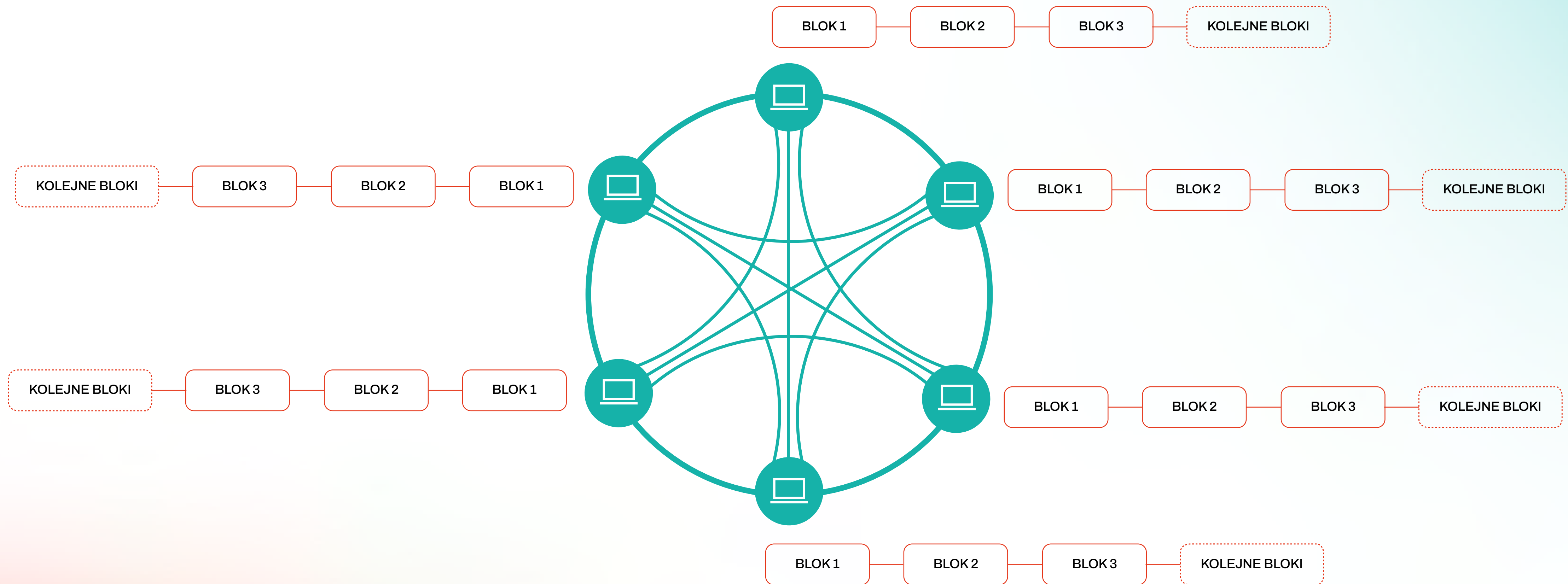
Kolejno tworzone bloki zawierają wynik funkcji skrótu utworzony z danych zawartych we wcześniejszym bloku. Dane są zapisywane chronologicznie i nie można ich zmienić po dodaniu.

5.

Aby dodać blok, wymagany jest konsensus sieci.

Gdy transakcje dodawane są do bloku, są również weryfikowane przez sieć.

Każdy węzeł przechowuje identyczną kopię łańcucha bloków.



Zdecentralizowanie oznacza zabezpieczenie prawdy

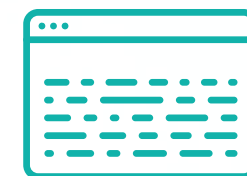
Model zaufania oparty na blockchainie jest odporny na manipulacje



Skalowalna, wspólna prawda

Nowa informacja zatwierdzana jest **konsensusem** węzłów, co pozwala na szybsze aktualizacje i wysoką odporność na **wiele równoczesnych zapytań**.

Zsynchronizowane kopie danych w kilku węzłach uzgadniają dodanie nowych bloków poprzez **konsensus**.



Brak nadpisywania i porządek

Dane dodawane są chronologicznie i **dopisywane** do rejestru poprzez wbudowane właściwości kryptograficzne. Nie możemy zmienić historii wpisów rejestru bez złamania systemu. To tworzy **rozliczalność**.

Chronologiczny zbiór danych z pełną historią zmian kluczy, pozwala na weryfikację ważności wcześniejszych podpisów.



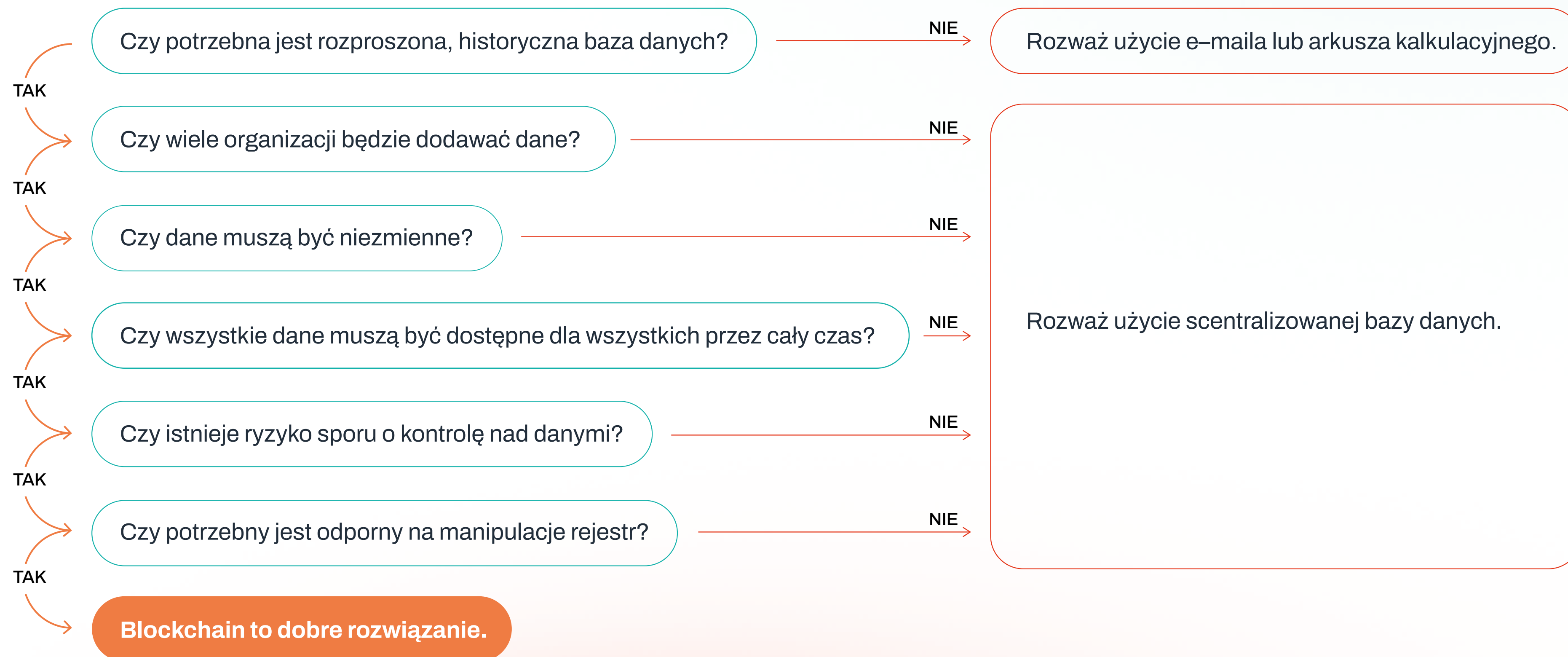
Odporność na nieuczciwe działania

Nawet jeśli jeden uczestnik działa w złej wierze, wspólna wersja prawdy zostaje zachowana. Blockchain zabezpiecza informacje przed przekłamaniami.

Brak pojedynczego punktu awarii. Infrastruktura jest zabezpieczona i odporna na cyberataki.

Blockchain nie zawsze jest najlepszym rozwiązaniem na każdy problem

Chociaż blockchain ma wiele potencjalnych zalet, ważne jest, aby pamiętać, że nie zawsze jest to najlepsze rozwiązanie i należy ocenić, czy w danym przypadku jego zastosowanie ma sens. Rozważając użycie blockchaina, zadaj sobie pytania:



Wykorzystuj blockchain tam, gdzie to ma sens

Blockchain idealnie odpowiada na potrzeby techniczne, biznesowe i społeczne dzięki odpornym i samonaprawiającym się mechanizmom, które mogą działać w trudnych warunkach. Wspiera otwarte platformy technologiczne i sprzyja rozwojowi konkurencyjnego rynku. Jednak technologia ta wiąże się także z wyzwaniami, takimi jak interoperacyjność, zarządzanie kluczami i niedojrzałość inteligentnych kontraktów.

Zamiast próbować na siłę dopasowywać blockchain do każdego możliwego zastosowania, **EBSI wykorzystuje blockchain i jego mocne strony** (niezmiennność, odporność na manipulację, decentralizację) **tam, gdzie ma to sens**. Dlatego właśnie EBSI **nie umieszcza żadnych danych osobowych w łańcuchu bloków** i stara się **minimalizować przechowywanie danych w blockchainie** w swoich zastosowaniach.

Właściwości blockchaina:

Tylko dopisywanie

Odporność
na manipulacje
i niezmiennność

Decentralizacja

Jak go wykorzystujemy:

Przypadki użycia wspierające dobro publiczne, poprzez opracowywanie specyfikacji we współpracy z ekosystemem i wspieranie ich wdrożenia

Nasze wartości:

Działania oparte na wartościach, zgodne z regulacjami i respektujące prywatność

Obalamy mity o blockchainie

Trzy istotne kwestie

1.

EBSI nie jest projektem blockchainowym.

Jesteśmy projektem Web3, który poszukuje sposobów wykorzystania technologii blockchain do wspierania zdecentralizowanych usług publicznych.

2.

Blockchain to nie tylko kryptowaluty.

Blockchain to rejestr zdecentralizowany. Może służyć wielu innym celom – jako repozytorium informacji zaufanych, do zarządzania łańcuchem wartości i wielu innych zastosowań...

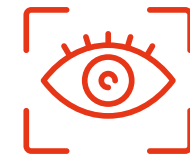
3.

Blockchain nie musi być energochłonny.

EBSI wykorzystuje mechanizm konsensusu Proof of Authority, który zużywa znacznie mniej energii niż Proof of Work czy Proof of Stake.

EBSI to technologia blockchain wdrażana w sektorze publicznym

Nasza działalność wykracza poza Weryfikowalne Poświadczenia (Verifiable Credentials). Oto kilka innych przykładów zastosowań:



Śledzenie i monitorowanie

Zapewnienie integralności i śledzenie zmian danych lub dokumentów; monitorowanie produktów w łańcuchu dostaw poprzez ich paszport cyfrowy.

Weryfikacja informacji

Przywracanie obywatelom kontroli nad ich poświadczeniami, np. dyplomami lub certyfikatami zawodowymi dla pracowników mobilnych, powiązanymi z ich tożsamością cyfrową, co znacząco obniża koszty weryfikacji i zwiększa zaufanie do ich autentyczności.



Zaufana wymiana danych

Usprawnienie wdrażania polityki UE i procedur zgodności pomiędzy agendami rządowymi, np. w zakresie obsługi wniosków o azyl lub wymiany numerów VAT dla produktów importowanych.

Zarządzanie prawami własności intelektualnej

Ułatwianie właścicielom praw sprawdzania i zarządzania własnością intelektualną oraz walka z przestępczością w tym obszarze. Odbywa się to m.in. poprzez ustanawianie rejestrów elektronicznych jako nowych kwalifikowanych usług zaufania, zgodnie z propozycją w rozporządzeniu UE dotyczącym tożsamości cyfrowej.



EBSI uczestniczy w tworzeniu rozporządzenia UE w sprawie tożsamości cyfrowej oraz portfela tożsamości cyfrowej UE.

