ANALIZA RYZYK

PROJEKT BEE COIN TOKEN

Wersja: 1.0
Data obowiązywania: 26.02.2026
Administrator: PartnerLedger OÜ (Estonia)

1. Cel dokumentu

Niniejsza Analiza ryzyk przedstawia ogólne kategorie zagrożeń związanych z funkcjonowaniem infrastruktury technologicznej projektu Bee Coin.

Dokument ma charakter informacyjny i służy zwiększeniu transparentności wobec użytkowników oraz partnerów.

Analiza nie stanowi porady inwestycyjnej ani oceny finansowej.

2. Charakter projektu

Bee Token / Bee Coin opisywany jest jako cyfrowa jednostka rozliczeniowa i płatnicza wykorzystywana w ekosystemie aplikacyjnym.

Projekt nie jest prezentowany jako instytucja finansowa ani platforma inwestycyjna.

Ryzyka opisane poniżej dotyczą głównie infrastruktury technologicznej i operacyjnej.

3. Kategorie ryzyk

3.1 Ryzyko technologiczne

Projekt opiera się na technologii blockchain oraz smart kontraktach.

Możliwe ryzyka obejmują:

- błędy kodu,
- awarie infrastruktury,
- zmiany w protokołach sieciowych,
- problemy skalowalności.

Administrator stosuje środki bezpieczeństwa, lecz nie gwarantuje pełnej odporności systemów.

3.2 Ryzyko regulacyjne

Otoczenie prawne dotyczące aktywów cyfrowych w UE i globalnie podlega zmianom.

Możliwe skutki:

- zmiana sposobu interpretacji tokenów,
- ograniczenia funkcjonalności,
- dodatkowe obowiązki compliance.

Projekt monitoruje zmiany legislacyjne, jednak nie ma wpływu na działania organów regulacyjnych.

3.3 Ryzyko operacyjne

Funkcje aplikacyjne mogą być wdrażane etapowo.

Ryzyka obejmują:

- opóźnienia w roadmapie,
- zmiany funkcjonalności,
- ograniczenia techniczne.

Opisane plany rozwoju mają charakter orientacyjny.

3.4 Ryzyko związane z podmiotami trzecimi

Niektóre elementy ekosystemu mogą być realizowane przez niezależnych operatorów.

Administrator nie kontroluje:

- regulaminów partnerów,
- jakości świadczonych usług,
- ciągłości działania systemów zewnętrznych.

3.5 Ryzyko rynkowe

Aktywa cyfrowe mogą podlegać zmienności i ograniczonej płynności.

Administrator:

- nie gwarantuje wartości tokena,
- nie promuje tokena jako inwestycji,
- nie zapewnia rynku wtórnego.

3.6 Ryzyko jurysdykcyjne

Dostęp do niektórych funkcji może być ograniczony w zależności od kraju użytkownika.

Zmiany prawa lokalnego mogą wpływać na sposób korzystania z ekosystemu.

Użytkownik odpowiada za zgodność z lokalnymi przepisami.

3.7 Ryzyko bezpieczeństwa

Mimo stosowania procedur AML Risk Framework i KYC Layer istnieje ryzyko:

- prób nadużyć,
- cyberataków,
- manipulacji technologicznych.

Administrator stosuje monitoring infrastruktury, lecz nie może wykluczyć wszystkich zagrożeń.

3.8 Ryzyko podatkowe

Kwalifikacja podatkowa aktywów cyfrowych może różnić się między jurysdykcjami.

Administrator nie zapewnia interpretacji podatkowej.

Użytkownik powinien samodzielnie ocenić skutki podatkowe.

4. Podejście do zarządzania ryzykiem

Projekt stosuje model risk-based approach, obejmujący:

- monitoring operacyjny,
- analizę ryzyka jurysdykcyjnego,
- procedury bezpieczeństwa infrastruktury,
- aktualizacje dokumentów compliance.

Szczegóły znajdują się w AML Risk Framework oraz Risk Disclosure.

5. Ograniczenia dokumentu

Analiza ryzyk:

- nie stanowi audytu finansowego,
- nie jest prognozą,
- nie daje gwarancji wyników.

Dokument opisuje ogólne scenariusze ryzyka w środowisku technologicznym.

6. Dokumenty powiązane

- Risk Disclosure
- AML Risk Framework
- Payment Token Notice
- VAT Neutrality Notice
- Regulamin serwisu

MACIERZ RYZYK

Skala oceny

Prawdopodobieństwo: Niskie, Średnie, Wysokie

Wpływ: Niski, Umiarkowany, Istotny

Kategoria ryzyka	Opis	Prawdopodobieństwo	Wpływ	Środki ograniczające (Mitigation)
Technologiczne	Błędy smart kontraktów, awarie sieci blockchain	Średnie	Istotny	audyty kodu, monitoring infrastruktury, aktualizacje
Regulacyjne	Zmiany przepisów UE dotyczących aktywów cyfrowych	Średnie	Istotny	EU Regulatory Shield, monitoring prawny
Operacyjne	Opóźnienia wdrożeń lub zmiany roadmapy	Średnie	Umiarkowany	etapowe wdrażanie funkcji, komunikacja roadmap
Jurysdykcyjne	Ograniczenia dostępu w wybranych krajach	Średnie	Umiarkowany	geofencing, AML Risk Framework
Rynkowe	Zmienność rynku aktywów cyfrowych	Wysokie	Umiarkowany	brak narracji inwestycyjnej, Payment Token Notice
Partnerów zewnętrznych	Ryzyka związane z operatorami obiektów	Średnie	Umiarkowany	rozdzielenie regulaminów partnerów
Bezpieczeństwa	Próby nadużyć lub cyberataków	Średnie	Istotny	monitoring 24/7, procedury bezpieczeństwa
Reputacyjne	Błędna interpretacja projektu	Średnie	Umiarkowany	Trust Center, dokumenty compliance
Podatkowe	Różnice interpretacyjne VAT	Niskie	Umiarkowany	VAT Neutrality Notice, separacja funkcji

Kategoria ryzyka	Opis	Prawdopodobieństwo	Wpływ	Środki ograniczające (Mitigation)
Technologii zewnętrznych	Zależność od dostawców infrastruktury	Średnie	Umiarkowany	redundancja usług, wybór dostawców