Nocturne

Słownik

Prywatność odnosi się do prawa jednostki do zachowania swojego życia, działań i danych w tajemnicy i bez ingerencji z zewnątrz. Dotyczy to ochrony informacji osobistych przed nieautoryzowanym dostępem, ujawnieniem lub udostępnieniem.

Anonimowość natomiast oznacza brak identyfikowalności jednostki. Osoba działająca anonimowo jest nierozpoznawalna i nie można jej zidentyfikować na podstawie dostępnych informacji.

Warunek konieczny ale nie wystarczający oznacza, że dany wymóg jest niezbędny, ale samo jego spełnienie nie gwarantuje osiągnięcia danego rezultatu.

Stealth address system na poziomie adresu Ethereum lub w ramach smart contractu, który pozwala na generowanie wielu niepowiązanych ze sobą "jednorazowych adresów".

Account abstraction rozwiązanie pozwalające na wykorzystanie smart contractu do zarządzania środkami bez konieczności transferu tych środków na dany smart contract.

Shielded pool rozwiązanie umożliwiające przyjmowanie i wydawanie środków bez ujawniania ich właścicieli.

Słowa kluczowe

> "account abstraction", "zero-knowledge proofs", "stealth addresses", "shielded pools", "compliance", "anonymous payments"

Problem

"Każdy powinien być w stanie:

- wykonać transfer swoich tokenów lub kryptowalut umieszczonych na blockchain bez ujawniania całości posiadanych środków na danym adresie,
- dokonywać zakupów bez ujawniania własnych nawyków zakupowych."

Dotychczasowe rozwiązania

1. EIP-5564 - system zgodny z definicją **Stealth address** jednak działający w oparciu o EOA (External Owned Accounts), posiadający niedogodności:
    - możliwe śledzenie transferowanych środków trafiających na wygenerowane adresy,

    - konieczność posiadania *ETH* na wygenerowanym adresie w celu umożliwienia dalszego transferu trafiających tam zasobów (ERC-20, ERC-721),
    - ciągłe pilnowanie braku powiązań pomiędzy adresami (jak i również wygenerowanymi adresami) jest trudne,
2. EIP-4337 - tzw. *account abstraction* rozwiązanie, które jest warunkiem koniecznym jednak nie wystarczającym w celu rozwiązania postawionego problemu

Proponowane rozwiązanie

Nocturne to implementacja mechanizmu **Shielded pool** z wykorzystaniem **Account abstraction**, w której uprawnione do wypłaty adresy to **Stealth address** dedykowane dla tego protokołu (nie są to adresy typu EOA).

Deponujący może wpłacić środki do **Shielded pool**, podając **Stealth address** odbiorcy jako właściciela, który zostanie wygenerowany. Odbiorca zostanie powiadomiony wówczas o środkach, którymi może zarządzać, udowadniając tożsamość w oparciu o **zero-knowledge proofs**.

Wartość dodana

1. Użytkownicy mogą nadal przesyłać środki w sposób anonimowy z powrotem na swój główny adres portfela bez tworzenia jawnego połączenia pomiędzy tymi adresami na blockchain, ponieważ tożsamość jest potwierdzona dzięki **zero-knowledge proofs**.
2. Użytkownicy mogą pokrywać opłaty za gas za pomocą wbudowanego mechanizmu płatności dzięki **Account abstraction** przy użyciu środków z dowolnego z **Stealth address**.
3. Autorzy projektu by być w zgodzie z przyszłymi regulacjami prawnymi i specyfiką protokołów dbających o prywatność i anonimowość, implementują ograniczenia co do ilości i częstotliwości wpłacanych środków oraz co do możliwości korzystania z protokołu dla adresów oznaczonych jako ryzykowne w oparciu o TRM.

Źródła:

1. Nocturne Docs
2. Nocturne Blog
3. An incomplete guide to stealth addresses
4. The Three Transitions
5. Should Ethereum be okay with enshrining more things in the protocol?

> Autor: @tomkowalczyk