Praca inżynierska

Wykorzystanie technologii blockchain do podpisywania autentyczności prac dyplomowych na uczelniach

Przez
Wojciech Szade

Politechnika Warszawska
Wydział Elektryczny
Informatyka Stosowana

Spis treści

1 Wstęp

W ostatnich latach dynamiczny rozwój technologii informatycznych znacząco wpływa na różne aspekty życia, w tym na edukację. Jednym z kluczowych wyzwań, przed którym stoją współczesne uczelnie, jest zapewnienie autentyczności i integralności prac dyplomowych. Tradycyjne metody weryfikacji stają się niewystarczające w obliczu rosnącej liczby oszustw akademickich oraz trudności związanych z manualnym sprawdzaniem dokumentów.

Istnieje pilna potrzeba wprowadzenia uniwersalnego narzędzia, które umożliwiłoby łatwą, szybką i skuteczną weryfikację autentyczności prac dyplomowych. Wdrożenie takiego systemu na wszystkich uczelniach, przyniosłoby korzyści zarówno studentom, jak i instytucjom edukacyjnym oraz innym podmiotom - takim jak pracodawcy. Uczelnie zyskałyby na reputacji i zaufaniu, jednocześnie upraszczając procesy administracyjne związane z weryfikacją dokumentów akademickich. Umożliwienie uczelniom w łatwy sposób podpisywania autentyczności prac w globalnym systemie umożliwiłby im zrezygnowanie z lokalnych rozwiązań, a studentom uprościłoby proces udowadniania prawdziwości swoich osiągnięć edukacyjnych.

Takie rozwiązanie musiałoby by być łatwe w użyciu i wdrożeniu, jednocześnie zapewniając wysokie bezpieczeństwo i integralność danych. W celu zagwarantowania trwałości i niezmienności danych system ten powinien być rozproszony.

2 Cel projektu

Celem projektu jest stworzenie kompletnego rozwiązania umożliwiającego:

- Utworzenie struktury typu blockchain przechowującej potrzebne dane.
- Podpisywanie autentyczności prac dyplomowych na uczelni poprzez dodawanie bloków do łańcucha.
- Synchronizacja łańcucha pomiędzy wieloma autoryzowanymi uczestnikami (uczelniami) zachowując jego identyczną wersję.
- Autoryzacja uczestników uprawnionych do podpisywania dyplomów.
- Stworzenie szkieletu serwisu do walidowania autentyczności prac dyplomowych przez nieautoryzowanych - dowolnych użytkowników.
- Stworzenie bezpiecznego połączenia do propagacji łańcucha bloków.

3 Proponowane rozwiązanie

Rozwiązaniem postawionego problemu składa się z dwóch warstw, **warstwy niepublicznej** oraz **warstwy publicznej**.

Warstwa niepubliczna to struktura łańcucha bloków, jak i sam łańcuch - jeden dla wszystkich uczelni oraz serwis umożliwiający tworzenie nowych bloków oraz ich propagację do sieci. W tej warstwie bardzo ważna jest odpowiednia autoryzacja użytkowników oraz zabezpieczenie przesyłu danych. W tej warstwie synchronizowana jest pełna kopia blockchaina i przechowywane są nowe bloki przez ich zatwierdzeniem w sieci. Serwis w tej warstwie nie łączy się z siecią zewnętrzną, a jest połączony jedynie między innymi autoryzowanymi użytkownikami, we współpracy z którymi dodaje nowe bloki do łańcucha.

Warstwa publiczna to serwis umożliwiający potwierdzanie autentyczności bloków, a tak właściwie sprawdzenie czy blok utworzony na podstawie podanych danych - identyfikatora pracy dyplomowej, jej tytułu i autora - istnieje faktycznie w bazie - łańcuchu bloków.
Warstwa ta korzysta z łańcucha bloków, ale nie ma żadnej możliwości jego rozszerzenia czy edycji. Serwis w tej warstwie udostępnia API, które uczelnia może zintegrować ze swoim rozwiązaniem obsługi studentów.

4 Plan pracy

1. Gruntownie zapoznać się z tematem blockhaina, zdobyć wymaganą wiedzę na temat zagadnienia, rozpoznać dostępne rozwiązania oraz ich wady i zalety. Wybrać najlepsze rozwiązania i opisać je, uzasadniając wybór. Zaproponować odpowiednie modyfikacje istniejących algorytmów i rozwiązań w celu najlepszego dopasowania ich do naszego zastosowania.
2. Zaproponować strukturę systemu, podział na warstwy, wykorzystywane technologie.
3. Stworzyć prototyp samego łańcucha blockchain, z prawidłową strukturą bloków.
4. Zaimplementować bezpieczną metodę komunikacji między uczestnikami.
5. Stworzyć implementację mechanizmu PoA, połączonego z łańcuchem. Zaimplementować system wybierania liderów, walidacji bloków, przesyłania ich między uczestnikami.
6. Dodać do systemu bezpieczną metodę walidacji użytkowników.
7. Stworzyć implementację drugiego systemu warstwy uzyskującego informacje z samego łańcucha.
8. Przetestować system na wielu maszynach.

5 Mechanizm konsensusu

Jako mechanizm konsensusu używany będzie Proof of Authority. Jest to rozwiązanie autentykacji nowych węzłów opierające się na zaufanych uczestnikach - w naszym przypadku uczelniach. W przypadku publicznych sieci blockchain można by je określić zcentralizowanym systemem, ponieważ zostanie zaufanym uczestnikiem jest trudne, a ilość ich jest ograniczona i niska, ale w przypadku naszego systemu rozwiązanie sprawdzi się to bardzo dobrze, a każda uczelnia będzie równym uczestnikiem sieci.
Nowe bloki w mogą tworzyć uczestnicy sieci, którzy w danym momencie są liderami. Kolejni liderzy wybierani są w sposób losowy i pozostają nimi tylko przez określony czas, po którym liderem zostaje kolejny uczestnik sieci.
Kiedy lider stworzy blok, mechanizm jego dodania do sieci przebiega następująco:

1. Propozycja bloku - lider tworzy nowy blok na podstawie pracy dyplomowej i jej danych,
2. Podpisanie bloku - lider podpisuje blok swoim prywatnym kluczem,
3. Rozpropagowanie bloku - blok jest rozsyłany do pozostałych uczestników sieci - walidatorów,
4. Weryfikacja bloku - pozostali uczestnicy sieci weryfikują podpis walidatora oraz poprawność bloku, po czym dodają go do łańcucha.

6 Struktura bloku

Blok składa się z nagłówka oraz ciała. Nagłówek przechowuje:

- Hasz poprzedniego bloku - zapewnia to chronologiczne powiązanie bloków i uniemożliwia modyfikację bloków.
- Znacznik czasu - czas utworzenia bloku.
- Korzeń drzewa Merkle - hasz utworzony na podstawie danych przechowywanych w ciele przy użyciu drzewa Merkle (drzewa skrótów).
- Podpis walidatora

Ciało przechowuje:

- Hasz PDF - hasz utworzony na podstawie pliku PDF pracy dyplomowej,
- Autora lub autorów pracy,

- Datę obronienia pracy,
- Nazwę uczelni,
- Nazwę wydziału.

Uczestnik będący liderem, nie musi stworzyć bloku w czasie bycia liderem. W standardowym wariancie Proof of Authority uczestnik taki został by oznaczony jako nieaktywny. Ale nasz system zakłada, że bloki wcale nie będą tworzone cały czas i nie każdy uczestnik powinien być w każdym momencie chętny do zostania liderem. Odpowiednie modyfikacje algorytmu mające na celu rozwiązanie tego zagadnienia opisane będą w kolejnych rozdziałach.
Jeżeli lider stworzy nieprawidłową lub niebezpieczną transakcję, to zostanie on wykluczony z listy członków. W naszym przypadku sytuacja taka mogłaby wystąpić tylko w wypadku przejęcia przez niepożądane osoby dostępu do systemu walidacji. W takiej sytuacji uczelnia musiałaby wyjaśnić sytuację, żeby wrócić do bycia członkiem systemu.
Zaletami systemu PoA są:

- Niska ilość obliczeń - w przeciwieństwie do drogiego systemu np. Proof of Work, wykorzystywanego w bitcoinie,
- Bazuje on na niskiej liczbie uczestników, przez co nowe bloki szybciej akceptowane są przez wszystkich uczestników i szybciej dodawane są do łańcucha.

Przykładem systemu korzystającego z PoA jest np. Microsoft Azure, a konkretniej Quorum Blockchain Service, będące komercyjną implementacją blockchaina, bazująca na Etherum i oferowaną klientom do różnych zastosowań.

7 Modyfikacje do mechanizmu konsensusu

Ze względu na specyfikę systemu należy dodać statusy, propagowane przez każde z uczestników.
Uczestnik sam wybierałby swój status i dzielił się tą informacją z każdym z uczestników.
Dostępne byłyby następujące statusy:

- Nieaktywny - niedostępny użytkownik, zarówno przekazujący taką informację lub nie propagujący żadnego statusu,
- Walidator - użytkownik, który nie ma żadnych bloków do dodania, nieubiegający się o pozycję lidera,
- Aktywny - użytkownik, który chce dodać blok i ubiega się o status lidera.

8 Bibliografia

Proof of Authority:
https://www.sciencedirect.com/science/article/abs/pii/S0065245819300245,
https://www.sciencedirect.com/science/article/pii/S1877050922000710,
https://medium.com/techskill-brew/proof-of-authority-or-poa-in-blockchain-part-11-blockchain-series-be15b3321cba,
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRLFs,