Wykorzystanie Ethereum do Budowy Zdecentralizowanej Aplikacji

Wojciech Korzeniowski

Instytut Informatyki
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska
http://www.ii.pw.edu.pl/

Streszczenie Opis smart kontraktów zdefiniowanych na platformie Ethereum. Przykład wykorzystania Ethereum do zrealizowania zdecentralizowanego systemu do głosowania. Koniec artykułu zostanie poświecony poszczególnym zagrożeniom wynikajacym z wykorzystania smart kontraktów wraz z konsekwencjami ich przeoczenia

Słowa Kluczowe: Ethereum · Smart kontrakt · Blockchain · Decentralized Application · DApp

1 Ethereum

Ethereum[1] jest zdecentralizowana platforma dla aplikacji które działaja dokładnie tak jak zostały zdefiniowane bez możliwości oszustwa, cenzury czy interwencji stron trzecich stworzona przez rosyjskiego programiste nazywajacego sie Vitalik Buterin. Ether jest kryptowaluta wykorzystywana na platformie Ethereum i pod wzgledem wartości rynkowej jest druga co do wielkości kryptowaluta na świecie. Na pierwszym miejscu plasuje sie Bitcoin[1].

To co wyróżnia Ethereum na tle Bitcoina to fakt iż pozwala on na definiowanie smart kontraktów. To z kolei umożliwia tworzenie nowego rodzaju aplikacji nazywanych DApp, czyli Decentralized Application, co w wolnym tłumaczeniu z jezyka angielskiego oznacza źdecentralizowana aplikacja". Nazwane sa tak ponieważ architektura blockchainu jest zdecentralizowana a smart kontrakt można traktować jako baze danych w której przechowywane sa dane aplikacji.

2 Smart kontrakt

Smart kontrakt jest kolejnym etapem rozwoju technologii blockchain. Można znaleźć tłumaczenia które opisuja smart kontrakt jako cyfrowy zapis umowy która w odpowiednich warunkach zrealizuje ustalona akcje. Z technicznego punktu widzenia jest to zbiór danych oraz funkcje które moga na nich operować i których wywołania sa jedynym sposobem na zmiane tych danych. Dodatkowo smart

[1] Według serwisu https://coinmarketcap.com/, stan na 2.06.2018

kontrakt może przechowywać Ether który jest kryptowaluta wykorzystywana w Ethereum. Dzieki temu wraz z wywołaniem funkcji kontraktu, wołajacy funkcje może przekazać Ether którym dysponuje jeżeli kontrakt tego wymaga. Ma to miejsce na przykład w grach hazardowych gdzie aby wywołać funkcje losu należy przekazać ustalona kwote Etheru. Smart kontrakty definiuje sie przy użyciu jezyka Solidity[2]

Istotna cecha która wynika z architektury blockchainu jest fakt iż smart kontrakt który został utworzony na blockchainie nie może zostać zmieniony. Jest to bardzo istotne ze wzgledu na bezpieczeństwo tworzonej aplikacji. Jeżeli popełnimy bład w definicji kontraktu nie mamy możliwości jego naprawy. Jedyne co można zrobić to utworzyć nowy kontakt i zaprzestać korzystania z jego starej wersji. Takie rozwiazanie nie zawsze jest satysfakcjonujace, szczególnie jeżeli do starej wersji kontraktu przypisana jest dana ilość Etheru a nie utworzyliśmy funkcji która pozwala na jego przekazanie na określone konto. Z drugiej strony istnienie funkcji która pozwala na wybranie całego Etheru z kontraktu może wzbudzić podejrzenia co do intencji jego twórcy.

2.1 System do głosowania

Przykładem smart kontraktu może być system do tajnego głosowania. Organizator głosowania tworzy umowe z osobami uprawnionymi do głosowania która pozwala Każdej z osób na oddanie dokładnie jednego głosu. Nastepnie, po zamknieciu głosowania, opcja która zebrała najwiecej głosów zostaje zwyciezca głosowania.

Zastanówmy sie najpierw jakie sa problemy w organizowaniu głosowania bez smart kontraktów. Przede wszystkim należy zadbać o to aby głos mogły oddać tylko osoby do tego upoważnione oraz aby każda z tych osób mogła oddać tylko jeden głos. Kolejnym problemem jest sposób w jaki głosy sa liczone. Jak powiedział Józef Stalin: Ńieważne, kto głosuje, ważne, kto liczy głosy."

Powyższe problemy w przypadku głosowań w Polsce rozwiazane sa przez Państwowa Komisje Wyborcza która pilnuje porzadku głosowania. Tworzone sa okregowe komisje wyborcze których odpowiedzialnościa jest sprawdzenie czy osoba głosujaca jest do tego uprawiona. Nastepnie komisja skrutacyjna liczy głosy po czym ogłaszany jest wynik głosowania.

Takie rozwiazanie wymaga istnienia tak zwanej zaufanej trzeciej strony. W przypadku wyborów w Polsce jest to PKW. Obywatele musza zaufać że w poprawny sposób i bez błedu komisja policzy głosy i ogłosi zwyciezce. Nie raz pojawiały sie różnego rodzaju kontrowersje co do sposobu przeprowadzania wyborów. Na przykład podczas wyborów samorzadowych 2014 opóźnione było ogłoszenie wyników. PKW tłumaczyła to awaria systemów informacyjnych jednak co bardziej podejrzliwi obywatele wyczuwali w tym spisek. Dodatkowo obywatele musza ufać że żadna z okregowych komisji wyborczych nie nadużyje swoich kompetencji i nie wykorzystaja kart do głosowania które nie zostały pobrane przez uprawionych do głosowania obywateli.

W przypadku głosowania zrealizowanego na smart kontraktach nie ma potrzeby istnienia zaufanej trzeciej strony. Można zdefiniować kontrakt którego

definicja jest ogólnie dostepna i każdy może sprawdzić w jaki sposób działa. Wymaganie iż każdy z uprawionych może zagłosować tylko jeden raz można zrealizować poprzez przekazanie każdemu z uprawionych jednego tokenu do głosowania który nie może być przekazany nikomu innemu. Osoba która wykorzystuje swój token do zagłosowania wywołuje odpowiednia funkcje na kontrakcie do głosowania w efekcie czego liczba głosów na dana opcje zwieksza sie. W każdej chwili można sprawdzić jaki jest aktualny stan głosowania, po jego zakończeniu wystarczy wywołać te funkcje i ogłosić wyniki.

Jedna z zalet realizacji systemu głosowania opartego na blockchainie jest jego transparentność. Ponieważ dane zapisane na blockchainie sa publicznie dostepne do odczytu każdy z zainteresowany może sprawdzić jak przebiegało głosowanie oraz jaki jest jego aktualny stan. Ponadto technologia blockchain gwarantuje że dane zapisane do blockchainu nie zostana zmienione wiec nie ma mowy o fałszowaniu wyników.

3 Token

Tokenem w świecie Ethereum nazywamy nowa "kryptowalute"która istnieje na blockchainie Ethereum. Istnieje przyjety interfejs tokenu o nazwie 'ERC20' który definiuje token o określonej liczbie gdzie każdy z tokenów jest równoważmy innemu.

Tokeny moga być wykorzystane do zbiórki pieniedzy co jest nazywane ICO (Initial Coin Offering) i jest odpowiednikiem określenia IOP (Initial Public Offering) znanego giełd papierów wartościowych. Przypuśćmy że właściciel startupu potrzebuje dofinansowania do swojego biznesu. Może on utworzyć token o dowolnej nazwie i totalnej liczbie tokenów. Nastepnie sprzedawać je za Ether. W ten sposób twórca pozyskuje Ether którym może płacić lub wymienić na inna walute. W zależności od przyjetej polityki ICO, Kupujacy token otrzymuje udziały w startupie lub możliwość wykorzystania tokenu w zamian za usługe realizowana przez biznes twórcy tokenu.

Za przykład może posłużyć serwis aukcyjny w którym za wystawienie produktu należy zapłacić tokenem. Ci którzy kupili token podczas ICO zorganizowanego przed uruchomieniem serwisu, moga go teraz wykorzystać lub sprzedać go innym którzy chca wystawić przedmiot na tym serwisie.

4 Komunikacja z siecia Ethereum

Sieć Ethereum składa sie z wezłów które komunikuja sie ze soba aby ustalić wspólna wersje blockchainu. Wezeł to serwer który posiada lokalna kopie blockchainu od poczatku jego istnienia wraz ze wszystkimi transakcjami i smart kontraktami które zostały na nim zapisane. Dodatkowo wezeł implementuje protokół JSON-RPC poprzez który nastepuje komunikacja klienta z wezłem. Jednym z bardziej znanych klientów jest klient napisany w jezyku JavaScript o nazwie

Web3.js[2]. Wykorzystujac go można stworzyć aplikacje działajaca w przegladarce która komunikuje sie bezpośrednio z wezłem Ethereum.

Inna możliwościa jest stworzenie własnego serwera który komunikuje sie z wezłem. Nastepnie aplikacja webowa komunikuje sie tylko z naszym serwerem bez bezpośredniej komunikacji z wezłem. Takie rozwiazanie może być wykorzystane w celu przyspieszenia aplikacji aby nie odpytywać wezeł o dane za każdym razem tylko przechowywać je w pamieci podrecznej na serwerze.

Funkcje zdefiniowane w smart kontrakcie można podzielić na 2 kategorie. Te które czytaja dane i te które je zmieniaja. Jako że dostep do danych z blockchainu jest publiczny i można stworzyć własny wezeł który jest pełna kopia blockchainu, dane można odczytać w każdej chwili. Inaczej jest w przypadku funkcji która modyfikuje stan kontraktu. Wynika to z faktu iż każdy z wezłów musi wywołać te funkcje aby potwierdzić czy inne wezły również ja wykonały i stan blockchainu sie zgadza. Operacja ta nazywana jest ustaleniem konsensusu pomiedzy wezłami. Fakt iż musimy wywołać ta funkcje na wszystkich wezłach powoduje że za wywołanie tej funkcji wywołujacy musi zapłacić. Waluta w której płaci sie za moc obliczeniowa wezłów w sieci Ethereum jest Gas który kupujemy za Ether.

Ilość Gasu potrzebnego do wywołania funckji jest proporcjonalna do jej złożoności obliczeniowej. Cena Gasu zależy od aktualnego obciażenia sieci oraz od tego czy chcemy aby nasza funkcja wywołała sie jak najszybciej czy nie. Wywołania funkcji, utworzenie smart kontraktu oraz transfer Etheru na inne konto nazywamy transakcja. Wszystkie transakcje trafiaja do puli transakcji (ang. Transaction Pool). Transakcje z puli sa akceptowane zaczynajac od tych za które jest ustalona najwieksza nagroda Gas Z puli brane sa kolejne transakcje zaczynajac od tych które z najwieksza opłata ponieważ te sa najbardziej korzystne dla kopaczy odpowiedzialnych za utrzymanie konsensusu.

Musimy jednak przyjać że wywołanie funkcji na każdym z wezłów w sieci nie może być za darmo.

`http://www.ethdocs.org/en/latest/`

5 Bezpieczeństwo

Dane aplikacji sa najcześciej centralnym punktem stworzonej aplikacji. Utrata danych może spowodować że aplikacja staje sie mniej wygodna w użytkowaniu[4] lub sprawa że użytkownicy traca zaufanie stracić zaufanie do aplikacji[3].

Innym z problemów jest wyciek danych[5]. W mojej opinii jest to gorszy scenariusz niż usuniecie danych ponieważ użytkownicy aplikacji (w przykładach z cytowanego artykułu - studenci) sa narażeni na Jeżeli natomiast nastapi wyciek danych zaufanie do twórców aplikacji maleje co może spowodować odpływ użytkowników.

Cieżko ocenić który ze scenariuszy jest gorszy. Usuniecie danych może sparaliżować prace użytkownika aplikacji lub nawet nieść konsekwencje prawne w

[2] https://github.com/ethereum/web3.js/

przypadku utraty wrażliwych danych które sa nie do odzyskania np. Dokumentacji podatkowych[6]. W przypadku utraty danych możemy przewidzieć jakie konsekwencje sie z tym wiaża. Inaczej jest gdy nastapi wyciek danych. Wyciek niesie niebezpieczeństwa które cieżko jest przewidzieć. Zdarzaja sie sytuacje w których serwis, świadomie lub nie, udostepnia czyjeś dane osobowe. W takim przypadku cieżko jest przewidzieć w jaki sposób takie dane zostana użyte. Jedna z takich wpadek zaliczyło Poznańskie Centrum Superkomputerowo-Sieciowe które pozwalało na pobranie imienia, nazwiska oraz adresu zamieszkana po podaniu numeru PESEL[7]. W niepowołanych rekach danie dane moga stwarzać realne niebezpieczeństwo dla dzieci które ogranicza tylko wyobraźnia atakujacego.

Wykorzystanie technologii blockchain pozwala ograniczyć wymienione powyżej zagrożenia ponieważ usuniecie danych z blockchainu jest niemożliwe. Cieżko też mówić o wycieku danych ponieważ dane zapisane na blockchainie sa publicznie dostepne. Oczywiście jeżeli chcemy przechowywać dane wrażliwe na blockchainie musza one być zaszyfrowane i możliwe do odczytu tylko dla odpowiednich osób. Jeżeli szyfrowanie zostanie zrealizowane błednie lub sam klucz szyfrujacy zostanie przejety przez atakujacego możemy mówić o wycieku danych.

Dodatkowo jak wspomniałem w rozdziale TODO, DApp może wykorzystywać tradycyjne bazy danych takie jak relacyjne czy NoSQL. W takim przypadku twórcy aplikacji musza brać pod uwage zarówno niebezpieczeństwa zwiazane z wykorzystaniem wybranej bazy danych jak i te wynikajace z użycia blockchainu które omówie w kolejnych podrozdziałach.

TODO [9]

5.1 Generowanie liczb pseudolosowych

[8]

6 Podsumowanie

Podsumowujac, system do głosowania wykorzystujacy blockchain nie wymaga istnienia zaufanej trzeciej strony co jest główna idea przyświecajaca smart kontraktom. Dzieki spisaniu zasad umowy w sposób jednoznaczny w interpretacji oraz gwarancji wykonania danych akcji po spełnieniu wcześniej przyjetych warunków możemy zawrzeć umowe z kimś komu nie musimy ufać bez potrzeby pośrednika w postaci notariusza.

Third Section

Fourth Level Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Literatura

1. Ethereum Homepage, `https://www.ethereum.org/`

2. Solidity - dokumentacj https://solidity.readthedocs.io/en/v0.4.24/
3. Awaria w Nazwa.pl – klienci stracili dane, także z backupów, https://niebezpiecznik.pl/post/awaria-w-nazwa-pl-klienci-stracili-dane-takze-z-backupow/
4. Teatr Współczesny zhackowany? Niestety to nie happening https://niebezpiecznik.pl/post/awaria-w-nazwa-pl-klienci-stracili-dane-takze-z-backupow/
5. Wyszukiwarki studentów, publiczna lista usterek i niebezpieczne punkty ksero, czyli uczelnianych wpadek cz. IV https://niebezpiecznik.pl/post/wyszukiwarki-studentow-publiczna-lista-usterek-i-niebezpieczne-punkty-ksero-czyli-uczelniany
6. Skutki utraty dokumentacji podatkowej http://www.ordynacjapodatkowa.pl/artykul,1679,5273,skutki-utraty-dokumentacji-podatkowej.html
7. Jak pozyskać dane osobowe i adresy dzieci z twojej okolicy? https://niebezpiecznik.pl/post/jak-pozyskac-dane-osobowe-i-adresy-dzieci-z-twojej-okolicy/
8. Predicting Random Numbers in Ethereum Smart Contracts https://blog.positive.com/predicting-random-numbers-in-ethereum-smart-contracts-e5358c6b8620
9. OpenZeppelin https://github.com/OpenZeppelin/zeppelin-solidity

7 Takie tam przydatne przykłady

Definition 1. *text*

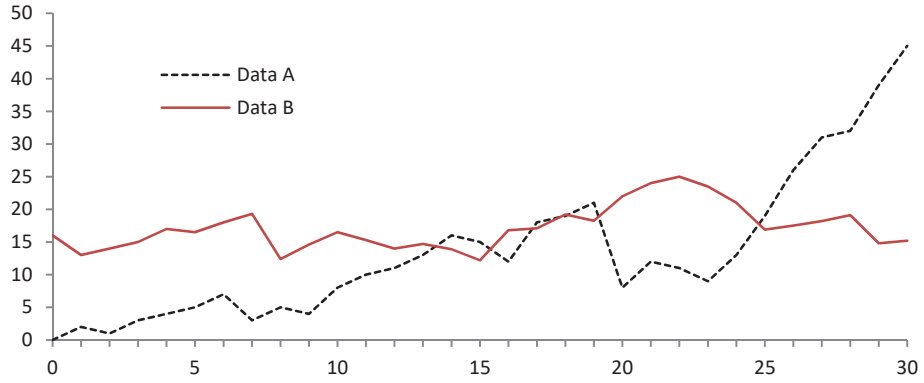
Case 1. text

Dowód. text

Widać na równaniu:

$$x + y = z \tag{1}$$

Please try to avoid rasterized images for line-art diagrams and schemas. Whenever possible, use vector graphics instead (see Fig. 1).



Rysunek 1. A figure caption is always placed below the illustration. Please note that short captions are centered, while long ones are justified by the macro package automatically.

Tabla 1 przedstawia że działa.

Tablica 1. Table captions should be placed above the tables.

Heading level	Example	Font size and style
Title (centered)	**Lecture Notes**	14 point, bold
1st-level heading	**1 Introduction**	12 point, bold
2nd-level heading	**2.1 Printing Area**	10 point, bold
3rd-level heading	**Run-in Heading in Bold.** Text follows	10 point, bold
4th-level heading	*Lowest Level Heading.* Text follows	10 point, italic