Przegląd możliwości istniejących sieci Blockchain

Projekt: “Przeprowadzenie prac badawczych i rozwojowych umożliwiających wdrożenie inteligentnego kontraktu opartego o technologię blockchain”

Autorzy:

- Blicharski Bartłomiej,
- Martin Morawiec

Kontekst: Wybrana sieć testowa będzie użyta do badań związanych z opracowywaniem metod Inteligentnych Kontraktów oraz opracowywaniem sposobów na umieszczanie danych w rozproszonej sieci blockchain. Zostaną zbadane od strony technicznej publiczne sieci blockchain oraz sposoby i możliwości jakie można uzyskać. Na tej podstawie powstaną stosowne wyniki badań, które pozwolą na wybranie sieci, która jest najbezpieczniejsza (najprawdopodobniej Ethereum powstałej w 2016 roku). W tym celu zostanie wykonany przegląd aktualnie dostępnych sieci i zostaną przetestowane ich możliwości pod kątem zastosowania Inteligentnych Kontraktów.

Spis treści:

Fundusze Europejskie Program Regionalny | Rzeczpospolita Polska | Śląskie. | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

1. Typy sieci blockchain

Sieć Blockchain to rozproszona baza danych, która stanowi rejestr transakcji pomiędzy klientami tej sieci. Pierwsza sieć blockchain powstałą ok. 2008 roku jako podłoże technologii Bitcoin - systemu transakcyjnego, który obecnie jest bazową światową kryptowalutą. Na jej podstawie pojawiły się kolejne kryptowaluty, a następnie kolejne rozwinięte sieci Blockchain różnych typów i niosące ze sobą różne funkcjonalności. Blockchain jest przełomową technologią, którą można przyrównać do powstania Internetu. Niektórzy twierdzą, że jest to sieć o dużo większym znaczeniu. Internet w tym zamyśle przyniósł wymianę informacji, natomiast Blockchain umożliwił przenoszenie wartości na niespotykaną dotąd skalę. Wiele źródeł i sposób użycia kryptowalut opartych o rozproszony rejestr wskazuje, że technologia ta jest w stanie zrewolucjonizować system płatności i zautomatyzować wiele procesów, dzięki pojawieniu się tzw. Inteligentnych Kontraktów. Obecnie Blockchain przeżywa swój rozwój i wyróżnia się trzy typy Blockchainów.

1. Blockchain Generacji I - rozproszony rejestr transakcji wartości P2P. Pojawił się na przełomie 2008/2009 roku, stworzony przez Satoshi Nakamoto, osobę lub grupę, która anonimowa pozostała do dziś. Na jego podstawie powstało wiele kryptowalut różniących się co do zasady założeniami. Pojawiły się takie kryptowaluty jak Litecoin, Dodge itp. które oferują inne możliwości
2. Blockchain Generacji II - rozproszony rejestr transakcji, Inteligentne Kontrakty. Tego typu Blockchain pojawił się na przełomie 2014/2015 roku. To wtedy pojawił się Ethereum, który jest zdecentralizowanym komputerem i umożliwia uruchamianie programów w formie kontraktów. Posiada inne właściwości niż Blockchain typu I - posiada warstwę kontraktów, która pozwala na wytwarzanie programowalnych transakcji (znanych jako Inteligentne Kontrakty).
3. Blockchain Generacji III - rozproszony rejestr transakcji

Inne właściwości sieci Blockchain:

Blockchain Centralizowany - np. Ripple, które powstało mniej więcej w podobnym okresie do Bitcoina, jednakże założeniem Ripple było umożliwienie błyskawicznych transakcji pomiędzy użytkownikami tej sieci. Technologia Ripple ....

Blockchain Prywatny - Technologia DLT (dystrybuowany rozproszony rejestr), dostępna prywatnie z prawami dostępu. Banki czy firmy mogą stawiać własny rejestr rozproszony prywatnie z prawami dostępu (umożliwia to m.in IBM Hyperledger Project). Są to blockainy kontrowersyjne. Jednakże z drugiej strony prywatne blockchainy dostarczają możliwości rozwiązania wewnętrznych problemów z efektywnością, bezpieczeństwem transakcji. Nie jest prawdopodobne, żeby prywatne blockchainy zrewolucjonizowały system finansowy, jednakże mogą one stanowić ciekawą alternatywę dla np. Projektów startupów, stanowiąc wewnętrzna alternatywę na rozwiązania transakcji finansowych w projektach informatycznych (zamiast używania modyfikowalnych klasycznych baz danych).

2. Przegląd sieci blockchain

Nazwa	Bitcoin [BTC]
Opis	Pierwszy Blockchain przeznaczony dla systemu transakcji w sieci Bitcoin. Dostarcza otwartą zdecentralizowaną bazę danych uporządkowanych bloków transakcji, które się odbyły. Komputery w sieci Bitcoin posiadają kopie pełnego rejestru bloków zawierającego wszystkie zaakceptowane bloki. Każdy pełny węzeł w sieci Bitcoin niezależnie utrzymuje pełną bazę blockchaina zawierającą tylko bloki zwalidowane przez dany węzeł. Kiedy większość węzłów posiada te same bloki w swoim blockchaine, to ten układ uważany jest za zgodny.
Możliwości	● Uporządkowany publiczny rejestr transakcji. ● Protekcja “podwójnego wydatkowania” i modyfikacji poprzednich rekordów ● Wszystkie transakcje są widoczne i publiczne. ● Transfer pieniężny bez zaangażowania “zaufanej” trzeciej strony ● Bloki potwierdzane przez PoW

Nazwa	Ethereum [ETC]
Opis	Pierwszy Blockchain drugiej generacji. Posiada możliwość tworzenia Inteligentnych Kontraktów.
Możliwości	● Inteligentne Kontrakty ● Obsługa domen ENS - rozbudowany serwis nazw, który pozwala na przypisanie domeny .eth dla portfela / kontraktu. Właścicielem domeny można zostać poprzez wygranie aukcji i zablokowanie kryptowaluty w nazwie minimum na rok. ● PoS (32 ETH) i PoW. Sieć hybrydowa. Cześć bloków

	walidowana za pomocą PoS, część jak dotychczas za pomocą PoW. ● Sharding - ● Na dzień 30.05.2018 - sieć jest w stanie obsłużyć ok. 20 transakcji na sekundę to sporo mniej w porównaniu z technologią kart kredytowych. W kolejnej wersji Ethereum wartość ta ma sięgnąć miliona/s. ● Możliwość podłączania się portfelem do zewnętrznej sieci. Klient nie potrzebuje ściągania całego blockchaina na lokalny komputer, aby rozpocząć transakcję. ● STARKs[1] - skalowalność, maskowanie transakcji, prywatność, zabezpieczenie przed kwantowymi komputerami. Najnowsza innowacja w prywatnosci transakcji stosowanej w finansach na blockchainie (szybkie skalowalne obliczenia i zatwierdzania). ZK Proof. ● Podział na kolejny Layer / Technologia Plasmy i Kanałów ● Tworzenie standardów typów tokenów np. ERC-20
	https://ethresear.ch

Nazwa	Aeternity [] Whitepaper: https://aeternity.com/aeternity-blockchain-whitepaper.pdf
Opis	Blockchain generacji III jest odpowiedzią na konieczność ułatwienia zintegrowania sieci z danymi z realnego świat i ułatwieniu wytwarzania aplikacji w oparciu o blockchain (webowych i mobilnych). Blockchain generacji III, który jest łatwy do skalowania, łatwy do opanowania i umożliwia wytwarzanie aplikacji poprzez pisanie skryptów. Blockchain jest napisany w języku erlang, który z założenia ułatwia pisanie rozproszonych systemów, jest wydajny przy czym stabilny. Technologia jest dostępna w open source, moduły mogą być bardzo łatwo implementowane w konsorcjach. Firmy mogą uruchamiać własne blockchainy Aeternity. Pomiędzy blockchainami możliwe są do wykonania “atomic swap” do reszty blockchainów platformy Aeternity. W Blockchainie głównym tokenem jest AE, które są “energią” dla każdej aplikacji zaimplementowanej na platformie. Wysoce skalowalne, funkcjonalne, weryfikowalne w łatwy sposób turing-complete inteligentne kontrakty. Łatwa olbrzymiej ilości transakcji wewnątrz kontraktu. Realizacja transakcji odbywa się poza głównym blockchainem w tzw. Sidechainach. Blockchain Aeternity zawiera maszynę Oracle, która zapewnia dostarczanie danych z realnego świata do blockchaina. Każdy

[1] ZK-Starks (Zero Knowledge Scalable Transparetn Argument of Knowledge)

	użytkownik może wysyłać zapytania do środowiska, a maszyna oracle dostarcza odpowiedzi. Zawiera przyjazny, zdecentralizowany i bezpieczny system nazw (podobnie do DNS).
Możliwości	• Blockchain 3 generacji • Możliwość tworzenia blockchainów

Dodatkowo zostały przeanalizowane inne sieci np. AION, EOS, IOTA inne. Obecnie sieci blockchain 3 generacji są w zbyt wczesnym stadium rozwoju, dlatego w celach realizacji projektu wybrany został Blockchain Ethereum.
Podpowiedź: Analizy sieci Blockchain powinny być aktualizowane w dalszych momentach projektu. Należy przyglądać się rozwojowi technologii.

3. Typy ICO

ICO - Initial Coin Offering Model

W ICO, kiedy sprzedaż tokenów kończy się, deweloperzy mają dostęp do wszystkich funduszy, kalkulują ile funduszy jest im potrzebnych do wyprodukowania MVP. Soft Cap w ICO odpowiada MVP. Deweloperzy po osiągnięciu w ICO “The Soft Cap” mogą rozpocząć pracę nad produktem i wydawać pieniądze na to na co wydaje im się konieczne. Jeżeli nie osiągną poziomu Soft Cap, muszą zwrócić pieniądze, ale jeżeli osiągną “Soft Cap”, nie dają żadnej gwarancji wykonania projektu. W ICO, kiedy zespół otrzymuje dziesiątki milionów dolarów, panuje dezorientacja w motywacji zaimplementowania projektu, albo aktywność spada znacznie.

DAICO - DAO + ICO Token Model

DAICO jest modelem finansowania, który łączy korzyści zdecentralizowanych autonomicznych organizacji (DAO) w celu utrzymania przejrzystej i bezpiecznej koncepcji ICO. Model ten pozwala wpłacającym na kontrolowanie wpłacania funduszy, a także daje możliwość głosowania za zwrotem wpłaconych środków, gdy zespoł nie realizuje projektu.

Jest ulepszeniem modelu ICO, który zawiera kilka aspektów związanych z zdecentralizowanymi autonomicznymi organizacjami (DAO). Idea stworzona przez Vitalika Buterina w styczniu 2018 roku, która oferuje większą kontrolę oraz bezpieczeństwo dla inwestorów. Umożliwia posiadaczy tokenów do zwrotów zaangażowanych środków wtedy kiedy nie są zadowoleni z prac wykonywanych przez deweloperów. Projekty, które zaimplementują koncept DAICO dają inwestorom gwarancję, że projekt zostanie zrobiony.

Ważne jest stałe informowanie inwestorów o postępie prac. DAICO jest inteligentnym kontraktem z mechanizmem, który umożliwia przesyłanie funduszy do projektu w zamian za tokeny, które oferuje dany projekt. Kiedy sprzedaż się kończy, kontrakt uniemożliwia pobieranie zainwestowanej kwoty przez kogokolwiek. W tym momencie zostaje uruchomiony kontrakt, który umożliwia deweloperom pobieranie określonej ilości Etheru / sekundę, które mogą zostać przelane na konta deweloperów. Początkowo limit ten jest równy 0, ale inwestorzy mogą głosować nad ustaleniem wielkości tego parametru.

Kontrakt DAICO zawiera kilka punktów z DAO. Decyzje o przekazywaniu funduszy odbywają się za pomocą demokratycznego systemu głosowania. Mechanizm pozwala na przydzielanie konkretnej części zebranych funduszy w czasie. Możliwość otrzymania zwrotu zainwestowanych pieniędzy (Inwestorzy mogą głosować za zwrotem pozostałych wartości jeżeli np. zespół programistyczny nie wykonuje zadań projektowych. W DAICO interesariusze mogą głosować nad zakresem prac deweloperskich, mogą zwiększać poziom spływającej gotówki do deweloperów, zmniejszać lub ogłosić chęć zwrotu.

Interesariusze mają więcej do powiedzenia podczas fazy developmentu projektu. Jeżeli są niezadowoleni z tego jak projekt się odbywa mogą odebrać resztę wpłaconych pieniędzy. Jest to zabezpieczenie przed tzw. SCAMem ICO, gdzie deweloperzy sprzedają token, a następnie zmywają się z rynku w momencie kiedy ICO się kończy, bez wyprodukowania żadnego produktu. Wielkość funduszy w ICO jest limitowana i kontrolowana. W modelu DAICO zespół jest zmotywowany do stworzenia projektu i przywołania projektu do życia, np. Dostarczenia produktu zgodnie z harmonogramem.

Deweloperzy posiadają dużą wartość tokenów, które stworzyli, potencjalnie mogą wpłynąć tylko na niewielki procent głosów. Inwestorzy muszą być edukowani - co jest kluczowe. Muszą rozumieć dlaczego cena konkretnego Tokenu rośnie lub spada aby prawidłowo głosować w DAICO. Najlepsze decyzje to między innymi te które bazują na faktach związanych z projektem, nie na emocjach związanych z ceną. Inwestorzy mogą również nie angażować się w głosowania i angażowania.

Prawidłowe DAICO powinno zaimplementować przykładowe mechanizmy takie jak:

1. Procentowy limit o ile wartość nagrody dla deweloperów może być podniesiona
2. Częstotliwość możliwości podnoszenia wartości na ETH/s (nie więcej niż raz na 2 tygodnie)
3. Tylko tokeny inwestora mogą być używane w głosowaniu, nie te, które są utrzymywane przez zespół
4. Interesariusze są informowani o planowanych pracach i planowanych wydatkach

5. Kiedy inwestorzy decydują o zamknięciu projektu, kontrakt DAICO uruchamia możliwość zwrotu reszty zaangażowanych pieniędzy, niszcząc tokeny trzymane przez deweloperów.

Ryzyka ICO:

1. Po zakończeniu sprzedaży tokenów, twórcy mają pełny dostęp do tokenów. Niebezpieczeństwo oszukania wpłacających.
2. Po zakończeniu sprzedaży, kiedy zebrano już dziesiątki milionów dolarów, zespół cierpi na brak motywacji do realizacji projektu.
3. Scentralizowane pozyskiwanie funduszy.
4. Niejasne warunki sprzedaży tokenów.

Zalety DAICO

1. Niezadowoleni inwestorzy mogą ustawić kontrakt na wypłaty i otrzymać zwrot pieniędzy
2. Środki są wypłacane mechanizmem rozłożenia wypłat w czasie. Motywacja zespołu jest zwiększona
3. Bezpiecznie przechowywane fundusze w zdecentralizowanej bazie.
4. Warunki sprzedaży tokenów są jasne i obsługiwane przez Inteligentny Kontrakt.

Frameworki:

https://aragon.one/core
https://eprint.iacr.org/2018/320
http://vault.io
https://github.com/aragon

Domeny
https://ens.domains
https://docs.ens.domains/en/latest/faq.html#how-was-the-minimum-character-length-of-7-chosen

Technologie
http://plasma.io
https://www.celer.network
https://www.perun.network
https://funfair.io

TypeScript
https://medium.com/buyethdomains/introducing-browseth-a-new-library-for-interacting-with-ethereum-795d18e7b87d
https://github.com/buyethdomains/browseth

Użycie sieci blockchain w głosowaniu:

1. https://cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-state-elections
2. https://www.cyberscoop.com/nasdaq-estonia-evoting-pilot/

PoS - Proof of Stake
https://www.rocketpool.net/files/RocketPoolWhitePaper.pdf