

Neo – Smart Economy

Raport 25.04.2019

by stokarz

Wprowadzenie

Jeżeli czytasz ten raport, raduj się. Oznacza to, że jesteś jednym z pierwszych. Należysz do wąskiej grupy anarchistów, śmiałków i buntowników, którzy nie zważając na liczne przeciwności, wątpliwe prawo i nieintuicyjne interfejsy graficzne, jako pierwsi adaptują i rozwijają technologię kryptowalut. Szczególnie dziś, po długim okresie ciężkiego rynku niedźwiedzia, gnani nową, asymetryczną w swej opłacalności sposobnością, mamy szansę stać się częścią potężnej fali wzrostowej wynikającej z rozwoju technologii i ludzkiej chciwości, która nadejdzie. Rynki, cykliczne w swojej naturze, oferują każdemu z nowych pokoleń właśnie takie okazje. Fortuny i majątki zbudowane przez pionierów, którzy do takowych fal podłączyli się w odpowiednim momencie, trwają przez dziesięciolecia. Dlatego gratuluję Ci, gdyż uczyniłeś pierwszy krok do osiągnięcia celu.

Krokiem drugim jest niezgubienie się w nieustannym napływie niepełnych informacji, oszustw, półprawd i naganiaczy. Cykle technologiczne wynagradzają pionierów, lecz dla większości z nich są całkowicie bezwzględne. Niewielu wytrwa w zaangażowaniu, część z nich pochłonięta zostanie przez zabójcze fluktuacje młodego rynku.

Informacja i wiedza są kluczem do przetrwania w kryptowalutach. Bez nich, zostaniesz oszukany, okradziony i wykorzystany. Dochodzenie do prawdy, wymaga czasu i zaangażowania. Na twoje szczęście właśnie to lubię robić. Dlatego prezentuje Ci dziś potężny zbiór wiedzy. Niech oświeci Ci drogę na tym kryptowalutowym dzikim zachodzie.

Zapraszam Cię do analizy i podsumowania kryptowaluty NEO, przez niektórych nazywanego „Chińskim Ethereum”.

Celem analizy było skupienie się na fundamentalnej architekturze NEO, obszerne przedstawienie i zrozumienie projektu, ocena projektu, a także wykrycie potencjalnych krytycznych wad, mogących w przyszłości zablokować dalszy rozwój NEO. Ze względu na obszerność projektów rozwijanych w ramach NEO, niektóre z pobocznych inicjatyw zostały w raporcie pominięte.

O autorze

Zajmuję się badaniem i analizowaniem świata kryptowalut. Prowadzę również portal edukacyjny o kryptowalutach. Fascynuję się nauką i technologią. Vires in numeris.

Opracowania i raporty możliwe są do realizacji na zamówienie. Przygotowuje raporty na temat konkretnych kryptowalut, a także wszelkich innych tematów związanych z rynkiem kryptowalut, jak np. opłacalność wprowadzenia danej usługi związanej z kryptowalutami na rynek.

Kontakt:

stokarzlol@gmail.com

Telegram: [@stokarz](https://t.me/stokarz)

Wszelkie raporty dostarczane przeze mnie nie stanowią porad inwestycyjnych. Nie jestem radcą inwestycyjnym, nie posiadam również uprawnień, aby takie porady udzielać. Analizy są jedynie moją opinią. Zabrania się dokonywania jakichkolwiek zmian w raporcie, bez mojej zgody.

Jeżeli chciałbyś wesprzeć moją pracę (wszelkie środki z napiwków przeznaczone są na opracowywanie dalszych raportów):



BTC: 3EPY1Ys9ojPdJGAbdC3fnjTzAetUPiAamP



ETH: 0xB92353CCeC318Bb0F5e0af050E08cE012846D8b8

Kluczowe wnioski:

- NEO posiada jedną z największych i najbardziej aktywnych społeczności
- Nad ekosystemem NEO pracuje kilkanaście zespołów deweloperów, rozproszonych głównie na Azję oraz Europę

- NEO jest całkowicie scentralizowanym blockchainem, co publicznie potwierdzają pracownicy i deweloperzy NEO. Dotychczas nie zostało zainicjowane przejście na model zdecentralizowany, choć było to zapowiadane od 2017 roku.
- Wszystkie z 7 węzłów walidujących (potwierdzających) wszelkie aktywności w sieci NEO są bezpośrednio (w przypadku 5 węzłów) lub pośrednio (w przypadku 2 węzłów) zależne od Rady NEO – głównego organu nadzorującego projekt NEO.
- NEO pomimo możliwości publicznego wglądu do sieci, ma cechy prywatnego blockchainu.
- Rada NEO posiada możliwość wprowadzenia dowolnych zmian w blockchainie NEO w każdej dowolnej chwili.
- Większość NEO posiadanych jest przez Radę NEO i giełdy kryptowalut, takie jak Binance, Bittrex i Bitfinex. W przypadku wprowadzenia możliwości głosowania za pomocą NEO na delegatów do węzłów walidujących, to właśnie te jednostki posiadać będą większość głosów (choć Da Hongfei zapowiada, że w przyszłości chciałby, aby ta sytuacja uległa zmianie).
- Wykorzystanie w blockchainie NEO algorytmu dBFT (Delegated Bantian Fault Tolerance) stwarza poważne problemy (obecnie nierozwiązane) w planowanej decentralizacji sieci i skalowalności blockchainu do zakładanych 10,000TPS, bez drastycznej reorganizacji fundamentalnej architektury systemu.
- Postacie takie jak Vitalik Buterin, sugerują nawet, że dBFT nie jest w stanie się skalować, bez pełnej centralizacji.
- dBFT (stanowiący hybrydę protokołów POS + pBFT) jest mniej bezpiecznym protokołem, aniżeli POW (Proof of Work). Konsensus między węzłami wymaga co najmniej 66.(6)% prawidłowo funkcjonujących węzłów.
- Jeżeli 3 z 7 węzłów (ang. Consensus Nodes) zarządzających blockchainem NEO przestaną działać, cały blockchain NEO ulega wyłączeniu.
- Finalność (ang. finality) po jednym potwierdzeniu z sieci, które ma trwać 15s. po wprowadzeniu dBFT 2.0 jest niemożliwa w zdecentralizowanym blockchainie.
- Kryptografia NEO opiera się na kryptografii funkcji eliptycznej – nie zostały więc dotychczas wprowadzone zapowiadane cechy odporności na łamanie szyfrów przy użyciu komputerów kwantowych
- Rzeczywista prędkość blockchainu NEO to 500TPS, a nie jak przedstawia to dokumentacja NEO – 1000TPS.
- Aktualne sygnatury kryptograficzne zastosowane w NEO, mogą prowadzić do rocznego wzrostu wagi blockchainu w wysokości nawet 900MB.
- NEO nie posiada kluczowych cech kryptowaluty i nie powinno być w takim zakresie traktowane. Nie jest również tokenem, gdyż dotychczas nie wprowadzono funkcjonalności (które opisane zostały w Whitepaper) takich jak prawo głosu w sieci, definiujących token. Proponowane nazewnictwo, które oddaje naturę NEO to własność cyfrowa. Aktualnie, jedyną działającą funkcją NEO to generowanie GASu.
- GAS działa jako zapłata za deponowanie smart contractów w sieci NEO, inne funkcjonalności, takie jak system opłat za transakcje w sieci, nie zostały dotychczas wprowadzone.
- Nadchodzące NEO 3.0 i dBFT 2.0 wprowadza wiele fundamentalnych zmian i popraw w blockchainie NEO i modelu NEO+GAS.
- Model NEO i GAS, biorąc pod uwagę sugestie i komentarze głównych inżynierów blockchain NEO z platformy Github, poddany zostanie dużym, dotychczas nie określonym zmianom.

- Wypowiedzi głównego architekta NEO Erika Zhanga wskazują na krytyczne błędy w aktualnym modelu. Wprowadzenie funkcji głosowania na węzły walidujące przy pomocy NEO mogłoby doprowadzić do tzw. blackhole, w przypadku którego utracony zostałby cały zasób wyprodukowane GASu.
- W NEO 3.0 rozważany jest nowy model inflacyjny GASu z powodu problemu wpadania NEO w martwe adresy, tzw. czarne dziury, podzielność NEO, a także braku inicjatywy ekonomicznej dla prowadzących węzły (co, według twórcy tego raportu, jest krytycznym uchybieniem w przypadku blockchainu, wprowadzającym zbyt duży czynnik zaufania i ekonomiczne inicjatywy poza sieciowe opierane na czynniku ludzkim).
- Aktualny współczynnik zaufania wymagany do korzystania z sieci NEO dyskwalifikuje tę platformę jako niezależny i zdecentralizowany, a tym samym trust-less blockchain do smart kontraktów. Cena 500 GAS za zdeponowanie smart contractu w łańcuchu głównym NEO, spowodowała, że wszelki rozwój NEO, a także ekosystemu wokół sieci, jest ściśle uzależniony i nadzorowany przez Radę NEO.
- Wykryto błąd, przez który za pomocą 20 GAS można zablokować całą sieć NEO
- Blockchain NEO posiada obecnie 130 (111 z nich to tokeny w standardzie NEP) zdeponowanych kontraktów. Ethereum z drugiej strony, posiada 1 200 000 kontraktów na łańcuchu głównym.
- Pomimo zapewnień Da Hongfei, CEO projektu NEO, przyglądając się, od fundamentalnej strony, blockchainowi rozwijanemu przez prywatną firmę zależną od NEO – Onchain oraz potwierdzając tym raportem, że NEO ma w rzeczywistości charakter prywatnego blockchainu, istnieje poważny konflikt interesu między tymi dwoma organami.
- Źródła z projektu DNA piszą, że do 2017 r. Onchain rozwijało częściowo NEO. Stanowi to duży znak zapytania w obliczu czwartej, prywatnej zbiórki kapitału.
- Analiza projektów przeprowadzających ICO na platformie NEO, wskazuje bezpośrednie lub pośrednie zaangażowanie członków NEO w owe projekty. Cel tego zaangażowania pozostaje domeną spekulacji.
- NEO posiada jedną z największych społeczności i placówek/organizacji pracujących nad ekosystemem NEO.
- NEO przeprowadziło 4 ICO – 3 publiczne i jedno prywatne z ramienia Onchain.
- Wszystkie pojawiające się problemy z kodem, rozwiązywane są na bieżąco.
- Jeżeli uda się przezwyciężyć wyżej wymienione problemy, NEO w formie pół-prywatnego blockchainu (jeśli zaimplementowany zostanie aktualny plan częściowej decentralizacji architektury weryfikacyjnej – szczególnie węzłów) ma szansę rozwinąć się, szczególnie, jako platforma blockchain dla gier i światów wirtualnych nowej generacji.

Ogólna ocena projektu:

6.5/10

Raport podzielony jest na trzy części. Część pierwsza stanowi wprowadzenie do NEO, część druga jest analizą fundamentalną technologii przez NEO wykorzystywanej. Natomiast część trzecia stanowi porównanie NEO do konkurencyjnych projektów, zagrożenia na przyszłość, problemy które NEO będzie

musiało przewyciężyć, a także plusy oraz minusy NEO. Na końcu zaś, znajduje się podsumowanie raportu. Serdecznie zapraszam!

NEO – Smart Economy

Część I

NEO¹ to rozproszona sieć, wykorzystująca technologię blockchain, cyfrową tożsamość oraz inteligentne kontrakty znane z Ethereum, w celu stworzenia czegoś, co przez twórców projektu nazywane jest Inteligentną Ekonomią. W ramach Inteligentnej Ekonomii (dalej IE) rozumie się stworzenie rozproszonej architektury sieciowej, pozbawionej czynnika zaufania, dzięki której tysiące użytkowników z całego świata, będzie w stanie wykorzystywać NEO do zapewnienia bezpieczeństwa swojej cyfrowej tożsamości. W skład IE wchodzi również: możliwość bezpiecznego zawierania inteligentnych kontraktów, cyfrowych aktywów możliwych do rozwijania w obrębie NEO – np. tokenów (obecnie w NEO wykorzystuje się dwa standardy tokenów – NEP5 będący odpowiednikiem ERC20 i NEP8 – odpowiednik ERC721), narzędzia SDK dla deweloperów i dApps. Szczególnie różne formy „tokenizacji” fizycznych aktywów i przeniesienie ich na platformę cyfrową są krokiem w dobrym kierunku (choć dokładnie to samo znamy już z Ethereum – tam też robione jest to na o wiele większą skalę, co zostanie zobrazowane w dalszej części).

Blockchain stanowi świetne narzędzie do przenoszenia cyfrowych reprezentacji fizycznych dóbr małym kosztem. Omija to przeszkody, nie tylko fizycznej odległości od zainteresowanych stron, lecz również bariery jurysdykcyjne. Przykład: tokenizacja konkretnej ilości fizycznego złota, zrobiona na pozbawionej czynnika zaufania, bezpiecznej sieci rozproszonej. Zamiast kupować fizyczne złoto, martwić się o liczne komplikacje prawne wynikające z różnych norm prawnych pośród państw przez które transportowane byłoby złoto, kupująca strona otrzymywałaby reprezentujące złoto tokeny, których posiadacz miałby prawo do określonej w kontrakcie ilości fizycznego złota. Jest to oczywiście przykład, a rzeczywista tokenizacja mierzy się z wieloma problemami, jak chociażby zapewnienie, że sieć jest całkowicie zdecentralizowana. Niemniej jest to ciekawe zagadnienie.

NEO w ramach IE dostosowuje swoją platformę również do nowej generacji gier opartych na blockchainie (CEO Da Hongfei² porównuje to do modelu grania przedstawionego w filmie „Ready Player One” – jednak według moich szacunków, przed NEO jeszcze długa droga, aby choć zbliżyć gry na swojej platformie do takiej formy).

Fundamentami IE NEO są również dwie kryptowaluty – NEO i GAS (choć w dalszej części udowadniam dlaczego NEO jako kryptowaluta traktowane być nie powinno). Mamy zatem do czynienia z modelem dwutokenowym. Każdy z tokenów, przynajmniej z założenia przedstawionego w Whitepaper NEO, pełni w całym ekosystemie określoną funkcję.

Ciekawostka: Wycena giełdowa NEO, nazywanego Ethereum Chin, w roku 2017 wzrosła o ponad 200,000%. Wynikało to, w głównej mierze, z fascynacji inwestorów Wschodnim rynkiem kryptowalut, a także fenomenalnym marketingiem NEO i trwającym w tamtym czasie potężnym rynkiem byka.

¹ <https://docs.neo.org/en-us/whitepaper.html>

² <https://firstblock.news/news/f7b9105a-a445-383d-adab-bbeedd90b73c>

Obecnie NEO zajmuje 17 miejsce³ w światowym rankingu kryptowalut. Jego wycena giełdowa to ponad \$10 USD, a kapitalizacja wynosi \$692M USD. W ciągu roku, w wyniku spadków całego rynku, straciło na wartości -86.02%.

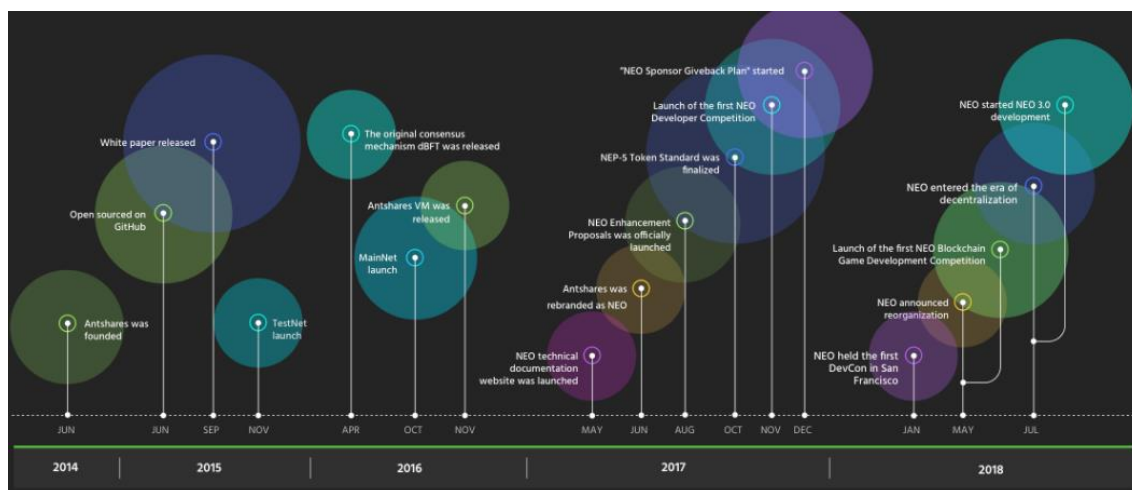
Struktura organizacyjna

NEO Foundation zarządzające NEO, jest oficjalnie organizacją non-profit (dlatego w raporcie pomijam analizę modelu biznesowego). Maksymalna podaż kryptowaluty NEO to 100M, z czego 65M jest obecnie na wolnym rynku, a kolejne 35M w rękach NEO Foundation. Według Whitepaper, pozostałe środki przeznaczone mają być na rozwój blockchainu NEO i inicjatyw wewnątrz ekosystemu. Maksymalna ilość NEO, jaką NEO Foundation może „odblokować” to 15M NEO w ciągu jednego roku.

NEO Foundation sprawują pełnię władzy decyzyjnej nad protokołem i ekosystemem NEO. W radzie nadzorczej zasiadają założyciele NEO – Da Hongfei i Erik Zhang, a także dwóch innych członków⁴. Fundacji NEO bezpośrednio podlegają dwa organy – NEO Global Development⁵ i NEO Global Capital. Pierwsza z wymienionych organizacji odpowiada za całość R&D (ang. research and development) i zajmuje się bezpośrednim, technicznym rozwojem NEO. NEO Global Capital z drugiej strony, piastuje funkcje licencjonowanego (na prawie Singapurskim) funduszu inwestycyjnego, służącego jako ramię inwestycyjne NEO, w celu zapewnienia komercyjnego wykorzystania side-chainów rozwijanych w obrębie NEO.

Faktem godnym zapamiętania jest również to, jakie spółki i projekty są bezpośrednio lub pośrednio związane z NEO (większość z nich została bezpośrednio założona przez Da Hongfei). Są to: NEO Foundation (zarządzające całym ekosystemem NEO), Onchain, Onchain Custodial, Ontology oraz inicjatywa od której wszystko się zaczęło – DNA (Distributed Network Architecture).

Historia NEO



Rysunek 1: Historia NEO 2014-2018

³ <https://coinpaprika.com/coin/neo-neo/>

⁴ <https://sludgefeed.com/neo-announces-new-organizational-structure/>

⁵ <https://lunardigitalassets.com/news/technology/2018/neo-the-chinese-ethereum-a-token-analysis/>

NEO założone w 2014 w Szanghaju, początkowo znane było pod nazwą Antshares. Z inicjatywą zbudowania NEO wyszło dwóch przyjaciół – Da Hongfei i Erik Zhang. Ufundowali oni również początkowe działania projektu. Niedługo potem, również w 2014 roku, Da Hongfei założył drugi z kluczowych w późniejszej historii projektów – prywatną firmę, zajmującą się rozwojem sieci rozproszonych i architektury blockchain, nazwaną Onchain. Onchain, w przeciwieństwie do NEO, to w pełni prywatna i komercyjna firma. Jak wykażę w późniejszej analizie, pomimo zapewnień, istnieje poważny konflikt interesów⁶ między systemem rozwijanym przez NEO a Onchain⁷, z ramienia którego założone zostało Ontology - projekt który początkowo wystartował jako token w standardzie NEP5 na platformie NEO.

Finansowanie projektu

Fundacja NEO (wtedy jeszcze Antshares) przeprowadziła trzy ICO (Initial Coin Offering – odpowiednik IPO w świecie kryptowalut). Jest to co prawda niecodzienne, gdyż zazwyczaj ICO przeprowadza się jeden raz, choć pod uwagę należy wziąć fakt, że w 2014-2016 roku kryptowaluty znajdowały się w zupełnie innym stadium rozwoju i rozpoznawalności. Niemniej trzykrotne zbieranie funduszy na ten sam projekt może być zastanawiające.

Pierwsze ICO⁸ przeprowadzono w październiku 2015 roku. W tym czasie zebrano ok. 2100 BTC⁹ o wartości \$550 200 USD. Crowd-funding odbył się na platformie WeAngel. Da Hongfei zaznaczył¹⁰, że celem było zobrazowanie (nie zostało podane komu dokładnie) jak blockchain może zostać wykorzystany do zbierania funduszy dla start-upów.

Drugie ICO¹¹ miało miejsce w kwietniu 2016 roku. W jego czasie zebrano, według szacunków, \$3.7-4M USD w Bitcoinie. Co więcej, między pierwszym a drugim ICO, zebrano dodatkowo \$4.5M USD w celu ufundowania dalszych działań Onchain. Ciekawe jest, że to drużyna Antshares zebrała owe środki na rozwój Onchain. Czyni to Onchain pośrednio zależnym (przynajmniej w początkowej fazie rozwoju firmy) od NEO (wtedy Antshares). Zastanawiające jest również to, że choć Onchain miało być prywatną firmą, według zapewnień Da Hongfei, pracującą nad zupełnie odmiennymi systemami, aniżeli NEO i nieprzedstawiającą konfliktu interesów, w artykule z projektu DNA, opisującym zakupienie przez chińską grupę Fosun dużej porcji akcji Onchain (być może właśnie to stanowiło część z domniemyanych \$4.5M USD od prywatnych inwestorów) podane jest, że Onchain pracował (przed 2017) nad NEO.¹²

Trzecie i ostatnie ICO¹³ odbyło się między 8 sierpnia, a 9 września 2017 roku, już po zmianie nazwy projektu z Antshares na NEO. Dzięki niemu, zebrano \$28M USD.

Podsumowując, NEO w fazie ICO, zebrało łącznie \$32 550 200 USD + \$4.5M USD (dla Onchain, od prywatnych inwestorów). Oficjalne komunikaty prasowe z Fundacji NEO podają, że po zamieszczeniu z

⁶ https://medium.com/@onchain_dna/understanding-the-onchain-neo-relationship-why-you-should-care-b8e69649ef98

⁷ <https://hackernoon.com/neo-onchain-and-its-ultimate-plan-dna-4c33e9b6bfaa>

⁸ <https://www.youtube.com/watch?v=eVawK0volwA&feature=youtu.be>

⁹ <https://blog.zerononcense.com/2018/10/04/neo-the-great-heist-an-analytical-research-case-study-pt-1-2/>

¹⁰ <https://bitcointalk.org/index.php?topic=1541424.0>

¹¹ <https://bitcointalk.org/index.php?topic=1571738.0>

¹² https://medium.com/@onchain_dna/chinas-fosun-group-buys-stake-in-blockchain-startup-5be79f741900

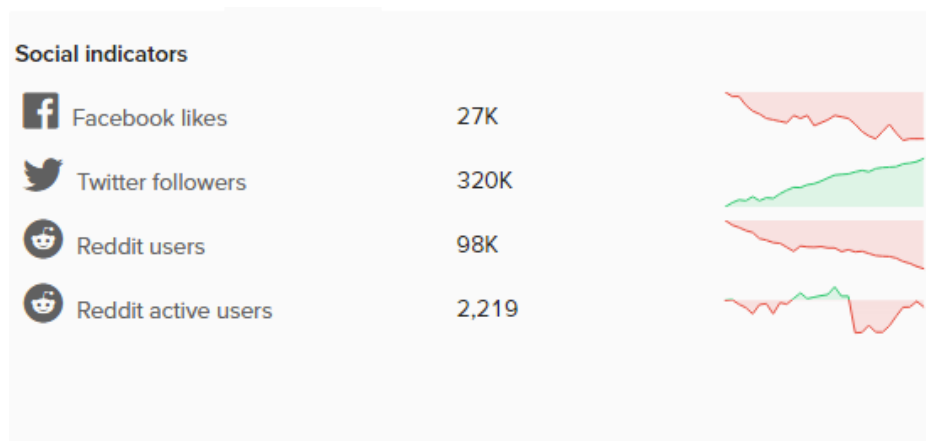
¹³ <https://icobench.com/ico/neo>

zablokowaniem ICO w Chinach w połowie 2017 roku, NEO zwróciło¹⁴ fundusze dla inwestorów uczestniczących w dwóch pierwszych ICO. Brakuje na to jednak dowodu, w postaci chociażby transakcji na blockchainie. Nigdy nie przedstawiono, dlaczego potrzebne były aż trzy ICO. Do dnia dzisiejszego pozostaje to słodką tajemnicą.

Schemat który znamy, wygląda następująco – NEO przeprowadza trzy ICO zbierając łącznie \$33M USD. Dodatkowo, w 2014 powołuje do życia prywatną firmę Onchain, mającą zajmować się zupełnie innymi systemami, aniżeli NEO. Jednak ich własne, oficjalne źródła, podają, że do roku 2017 Onchain pracował nad rozwojem NEO. Można więc założyć, że NEO przeprowadziło więc łącznie 4 ICO – trzy z nich publiczne i jedno prywatne z ramienia Onchain (które należy do NEO), zbierając łączną kwotę w wysokości \$37M USD.

Społeczność

Rzeczą wartą zauważenia jest jak bogata i duża jest globalna społeczność NEO. W tym aspekcie jestem naprawdę pod wrażeniem.



Rysunek 2: NEO w mediach społecznościowych

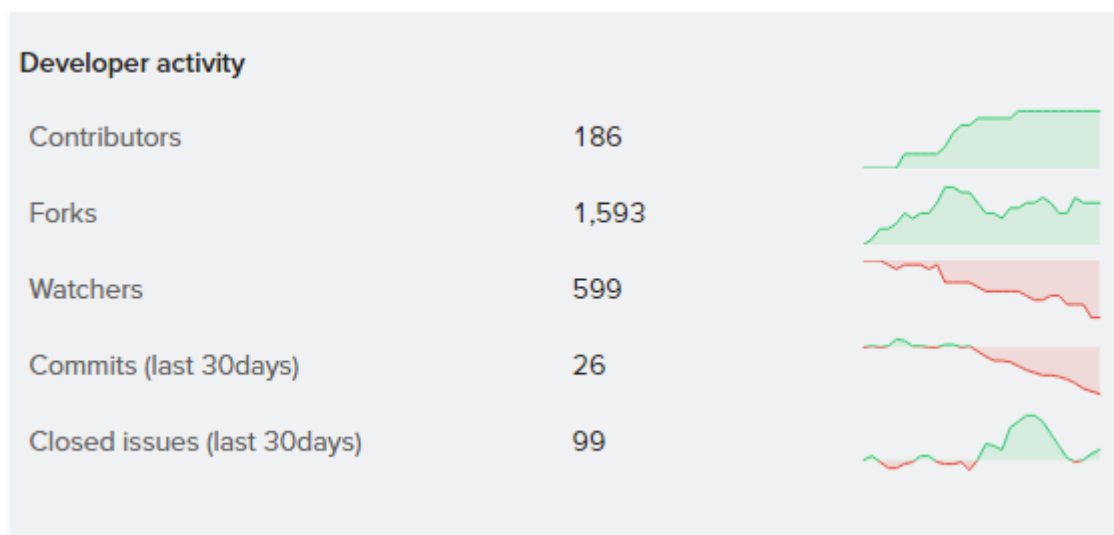
NEO rozwijane jest również przez sporą liczbę sub-organizacji i grup międzynarodowych. Pełna lista, a także adresy do poszczególnych inicjatyw znajdują się poniżej:

¹⁴ <https://www.ccn.com/china-bans-ico-successfully-completed-icos-to-return-funds-to-investors>

- CoZ (City of Zion): <https://cityofzion.io>
- NEL (NewEconoLabs): <https://nel.group/index-En.html>
- NeoResearch: <http://neoresearch.io>
- NSPCC (NEO Saint Petersburg Competence Center): <https://nspcc.ru/en/>
- NNT (NEO NEWS TODAY): <https://neonewstoday.com>
- Red4Sec (Security partner): <https://red4sec.com/en>
- NEO-ONE: <https://neo-one.io>
- neow3j: <https://github.com/neow3j>
- Keymakers: <https://neo-jp.org/en/>
- NEXT: <https://neonext.club>

Rysunek 3: Grupy deweloperskie NEO

Tak bogata liczba grup deweloperskich owocuje bardzo sprawnym rozwiązywaniem problemów w blockchainie NEO oraz wysoką aktywnością nad Githubie:



Rysunek 4: Wykaz aktywności na Githubie NEO¹⁵

Roadmap projektu – NEO 3.0 i dBFT 2.0

Wielkimi krokami zbliża się planowana od ponad roku aktualizacja całej fundamentalnej architektury. Protokołu, na bazie którego dochodzi do konsensusu w obrębie blockchainu NEO – mowa tutaj o protokole dBFT, który zostanie szczegółowo omówiony w późniejszej części dokumentu, a także samego blockchainu. Erik Zhang, współzałożyciel NEO i główny architekt oprogramowania, w jednej ze

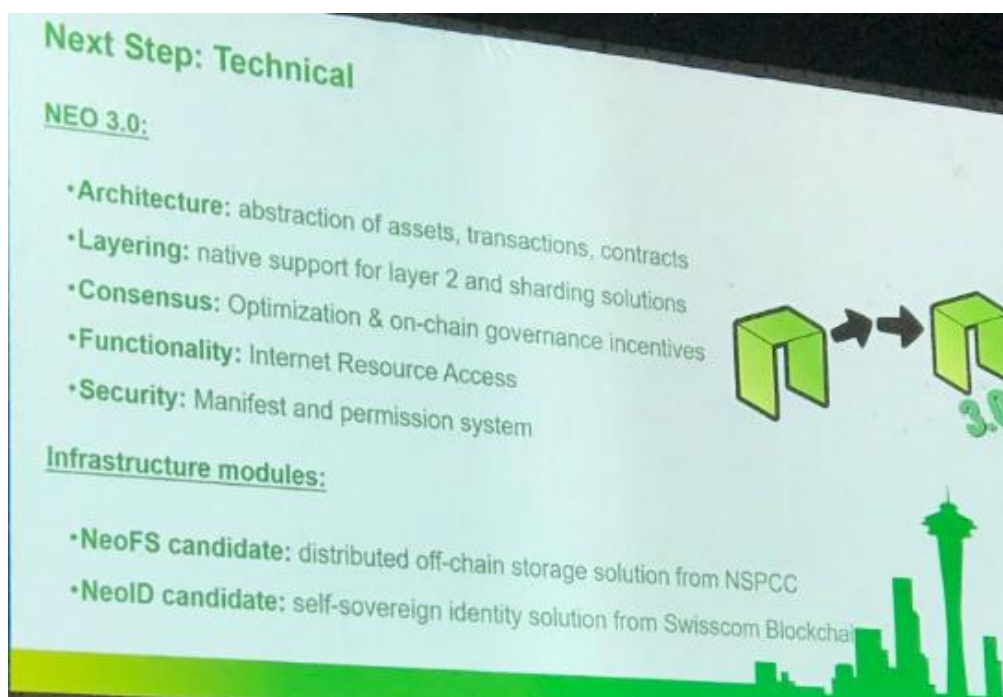
¹⁵ <https://github.com/neo-project>

swoich licznych prezentacji¹⁶ na ten temat, a także w otwartych dyskusjach deweloperskich na platformie Github, wymienia filary na których opierać się ma nowy system.

- Niezawodność systemu, nieuleganie awariom.
- Zwiększone (i tańsze) możliwości przechowywania danych bezpośrednio na głównym łańcuchu.
- Zwiększenie ilości transakcji na sekundę.

Każdy z tych aspektów zostanie omówiony później, gdyż istnieją poważne wskazania, że NEO nie da rady osiągnąć tych zamierzeń, nie zmieniając od samych podstaw wszystkich zasad funkcjonowania swojej sieci.

Erik Zhang dodaje również, że chciałby przenieść wszystkie aplikacje budowane obecnie na tzw. drugiej warstwie ekosystemu (rozwiązania off-chain) bezpośrednio na główny łańcuch NEO. Chce radykalnie uprościć wiele aspektów obecnego protokołu NEO (nie zostało wymienione co dokładnie), tak aby przeniesienie wszystkich na główny łańcuch było możliwe.



Rysunek 5: Zmiany w NEO 3.0¹⁷

Planowane jest także uproszczenie architektury cyfrowych „własności” (ang. assets). Obecnie różnią się one zasadniczo w kwestiach kodu w stosunku do zwykłych smart contractów NEO. Zhang pragnie reorganizować tę część systemu, tak, aby od tego momentu, wszystkie cyfrowe własności w obrębie NEO – np. różne hybrydowe typy tokenów, były reprezentowane jako inteligentne umowy.

Kolejną huczną zapowiedzią jest wprowadzenie NEOFS – propozycja, aby zbudować rozproszoną architekturę chmurową, podobną do tej znanej z SiaCoin albo polskiego projektu Golem. Celem takiego przedsięwzięcia byłoby przede wszystkim drastyczne obniżenie kosztów składowania danych w obrębie blockchainu (jako rozwiązanie tzw. second layer). Niemniej, choć takie są plany, doświadczenie z takimi systemami rozwijanymi przez wyżej wymienione projekty, pokazuje, że jest to rzecz niezwykle trudna. Co więcej, ogromny problem stanowi znalezienie potencjalnych klientów do takich usług, gdyż aktualnie zdecydowanie bardziej opłacalne jest wykorzystanie zwykłej chmury obliczeniowej, np. AWS

¹⁶ <https://www.newsbtc.com/2019/03/03/zhang-neo-3-0/>

¹⁷ <https://www.ccn.com/neo-da-hongfei-top-crypto-blockchain-2020>

od Amazon. Wątpliwe pozostaje również, żeby rozproszona chmura NEO była rzeczywiście – rozproszona. Ich aktualna centralizacja projektu (o czym mowa jest w późniejszych akapitach), jasno pokazuje, że NEO decentralizacją zainteresowane jest jedynie na papierze, bądź w długoterminowych planach.

Jednym z problemów, z którym mierzy się NEO, są wysokie opłaty za zdeponowanie Smart Contractów, co czyni NEO gorszym wyborem aniżeli chociażby Ethereum. To również ma ulec zmianie w NEO 3.0 ¹⁸

Konkretna data wdrożenia NEO 3.0 oraz zmiany planowane w ramach dBFT 2.0 pozostają w obszarze spekulacji (choć pierwsza implementacja dBFT 2.0 ma zostać wprowadzona w maju 2019, jednak nie opublikowano jak dotąd kompletnego kodu). Prace na platformie Github nad tymi właśnie udoskonaleniami systemu trwają nieprzerwanie od połowy 2018 roku. Między deweloperami omawiane są różne propozycje, jednak nic nie wskazuje na to, aby dotychczas wykrystalizowała się jasna wizja, czym NEO 3.0 ma być, oprócz zmian w protokole i kilku ulepszeń.

Wizja długofalowa

Da Hongfei nie spoczywa na laurach. Jego długofalowa wizja NEO jest jasna¹⁹. Do 2020 roku (choć możemy spokojnie mówić o dłuższym okresie, gdyż takie założenie jest niemożliwe do zrealizowania) chciałby, aby NEO stało się kryptowalutą TOP 1. Co więcej, swoją wizję obrazuje odwołując się do protokołu TPS/IP i HTML. Chciałby, aby NEO zajęło właśnie takie miejsce w przyszłości. Aby stało się dla zdecentralizowanych aplikacji tym czym wyżej wymienione protokoły są dla internetu.

Na chwilę obecną są to jedynie zapowiedzi bez pokrycia. NEO procesuje maksymalnie 500TPS, a dokładne zbadanie ograniczeń technicznych dBFT oraz typ używanych obecnie sygnatur kryptograficznych pokazują, że plany te nie są na tą chwilę możliwe (patrz: sekcja analizy dBFT).

¹⁸ <https://neo.org/blog/details/4091>

¹⁹ <https://www.ccn.com/neo-da-hongfei-top-crypto-blockchain-2020>

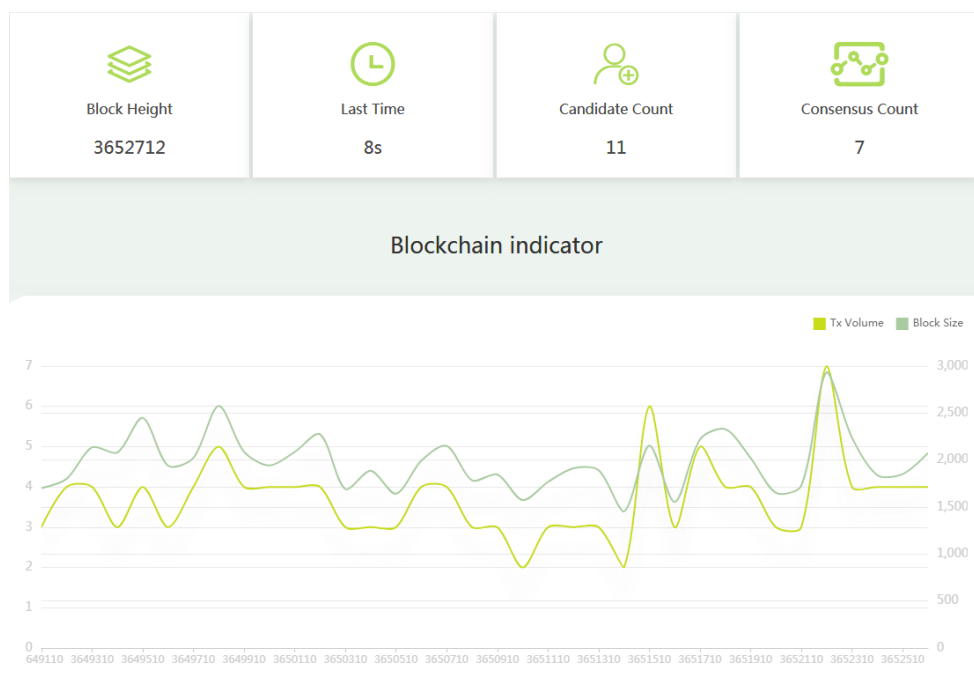


Rysunek 6: Nie pierwszy raz NEO pełne jest hucznych zapowiedzi

Część II

Zostaliście już wprowadzeni do NEO, jego struktur, a także wizji długofalowej. Poznaliście czym NEO jest oraz czym chciałoby się stać. W części drugiej tego raportu, zajrzę, dosłownie, pod spódnicę NEO, odkrywając i obszernie analizując fundamentalne zasady działania protokołów, blockchainu który NEO wykorzystuje i dowiecie się jakie krytyczne zagrożenia wynikające ze specyfiki używanej technologii, mogą zagrozić NEO w realizowaniu dalszych planów. Omówię również dwutokenowy model na bazie którego NEO funkcjonuje, poznacie również jakiego standardu tokenów używa.

Blockchain NEO i Smart Contracty



Rysunek 7: Jak widzicie, blockchain NEO ²⁰nadzoruje jedynie 7 węzłów²¹ (zwanym jako Consensus Nodes)²²

Pomimo że, Whitepaper²³ NEO, stanowiący najważniejszy dokument projektu stwierdza, że NEO jest zdecentralizowane, nie mogłoby to być dalsze od prawdy.

Cały blockchain NEO zarządzany jest przez 7 węzłów walidujących (Consensus Nodes), które w całości należą do NEO Foundation, lub są po jego pośrednim nadzorem – 5 nodów należy do NEO F., jeden do ich partnera, a ostatni zarządzany jest przez City of Zion, międzynarodową grupę deweloperów NEO zarządzaną przez NEO F.

NEO może przetworzyć 500TPS²⁴, taki jest też limit ustawiony w kodzie jednego bloku (a nie 1000TPS jak powszechnie się przyjmuje). Blockchain NEO bazuje na kryptografii funkcji eliptycznej, co czyni go nieodpornym na łamanie szyfrów przez przyszłe komputery kwantowe. Kryptografia kwantowa nie została zaimplementowana w NEO, nie ma również planów na wprowadzenie jej w planowanym NEO 3.0. Jest to zastanawiające, gdyż niektóre strony informacyjne o NEO, nadal podają, że jest ono QS (Quantum Secure). NEO było również niejednokrotnie promowane²⁵ jako QS, co możemy uznać za zwykłą nieprawdę, lub niedoinformowanie (w podanym artykule znajdują się zresztą inne błędy, jak chociażby to, że NEO może przetworzyć 1000TPS).

²⁰ <https://neo.org/consensus>

²¹ <http://monitor.cityofzion.io/>

²² <https://neotracker.io/>

²³ <https://docs.neo.org/en-us/whitepaper.html>

²⁴ https://neoresearch.io/assets/yellowpaper/yellow_paper.pdf

²⁵ <https://hackernoon.com/nep-5-neos-answer-to-ethereum-erc-20-tokens-69d9b082c9e1>

Price	\$11.0348
Coin Details	proof: proof of stake
Category	platform, blockchain, platform
Technology	blockchain
Features	quantum secure, crosschain

Rysunek 8: Błędne twierdzenie, jakoby NEO było QS – strona myli się również w rodzaju algo. użytego w NEO – dBFT to hybryda POS + starszego pBFT znanego z prywatnego blockchainu Hyperledger

Całkowita centralizacja blockchainu NEO jest ogromną czerwoną flagą. Nawet pracownicy²⁶ przyznają otwarcie, że NEO jest scentralizowane. Oficjalnym powodem mają być wymagania deweloperskie i potrzeba utrzymania sieci w spójności do czasu wprowadzenia kolejnych węzłów. Jednak od 2017 roku utrzymuje się, że NEO stanie się zdecentralizowane. Choć przedstawiono liczne dokumenty²⁷, to²⁸ takie, jak pokazuje skan blockchainu zaprezentowany powyżej, nic w tej materii nie uległo zmianie.



deanpress commented on Jul 10, 2018 • edited ▼

One of NEO's main attracting powers was always that if decentralization would be introduced, consensus nodes can be run by parties without any direct incentives from transaction fees. Consensus nodes would benefit from other factors such as funding/exposure/contributing to ecosystem, and the blockchain fees would be distributed only to NEO holders (not consensus nodes). NEO holders would also be in control deciding over the blockchain's fees.

Rysunek 9: Github - deweloper NEO przyznaje, że NEO jest scentralizowane

Jest to niezwykle istotne z kilku powodów. Po pierwsze, kryptowaluty z założenia, czystej definicji, muszą być zdecentralizowane. Ukrywanie prywatnego blockchainu zarządzanego w całości przez jedną fundację, pod pozorem zdecentralizowanej sieci, stwarza ogromne zagrożenie dla deweloperów budujących swoje rozwiązania na NEO, lecz również jest czystym kłamstwem wobec inwestorów. **NEO, przez swoje całkowite uzależnienie decyzyjne od Fundacji, ma w rzeczywistości charakter prywatnego blockchainu, możliwego do publicznego wglądu.** W NEO 3.0 nie planuje się tego zmienić, a proces wprowadzania nowych Consensus Nodes stoi w miejscu.

Do osiągnięcia konsensusu w obrębie sieci NEO wymagane jest minimum 66.(6)%²⁹ sprawnych węzłów. Przypomnijmy, że 5 z 7 węzłów kontrolowane jest bezpośrednio przez Fundację NEO. Sprawia to, że blockchain NEO jest całkowicie zależny od Fundacji, której deweloperzy mogą w każdej dowolnej chwili zmienić wszelkie reguły systemu. Na tą chwilę, NEO jest zatem prywatnym blockchainem. Dopóki nie zostanie wprowadzony proces szerokiej decentralizacji, a węzły walidacyjne operowane nie będą

²⁶ <https://medium.com/@MalcolmLerider/response-to-baseless-fud-9b7e5e2e4444>

²⁷ <https://medium.com/neo-smart-economy/how-to-become-a-consensus-node-27e5317722e6>

²⁸ <https://medium.com/neo-smart-economy/neo-consensus-node-page-updated-to-speed-up-decentralization-progress-556db7f76de8>

²⁹ <https://medium.com/@neospcc/task-distribution-over-consensus-nodes-42f1349442ad>

przez niezależne trzecie strony, NEO pozostaje całkowicie scentralizowane i nie powinno być rozważane w innych kategoriach.

Ważną rzeczą jaką należy dodać w kwestii uczciwego wyboru Consensus Nodes - planowane było wprowadzenie możliwości głosowania za pomocą tokenu NEO na delegatów. Dałoby to możliwość demokratycznego wyboru delegatów, którzy oferowali by jakąś inicjatywę ekonomiczną, np. tanie transakcje. Niemniej, znacząca większość NEO posiadanych jest przez giełdy: Binance, Bitfinex oraz Bittrex i Fundację NEO³⁰. Sprawiałoby to, że w przypadku wprowadzenia modelu głosowania, jaki znamy chociażby z LISK (z modelem dPOS) Fundacja NEO wraz z giełdami, miałaby niemożliwą do pokonania hegemonię decyzyjną w kwestii wyborów CN. Tworzy to praktyczny monopol na decyzyjność o dalszym rozwoju projektu – jeżeli zasób NEO nie zostanie również poddany decentralizacji, nie ma tu miejsca na nazywanie NEO publicznym blockchainem.

Kryptowaluty, wykazujące się pełną, jak w przypadku Bitcoina, bądź chociaż częściową – Ethereum, Monero, Dash, decentralizacją zawsze posiadają pewien mechanizm zapewniający inicjatywę ekonomiczną do posiadania pełnych węzłów. Transakcje w Bitcoinie potwierdzane są przez górników, a protokół POW (Proof of Work) zapewnia im inicjatywę finansową za zabezpieczanie sieci. Jednocześnie użytkownicy muszą również zapłacić drobną opłatę (Bitcoin, Ethereum) za wysłanie transakcji. Ten mechanizm powoduje, że nieopłacalne staje się spamowanie blockchainu (który przecież nie jest w żadnym wypadku wydajną bazą danych) zbędnymi transakcjami – gdyż jest to kosztowne.

Transakcje w obrębie NEO są natomiast darmowe. Zadziwiające? Nie, gdyż wiemy już, że NEO jest prywatnym blockchainem o jedynie pozornej publiczności. Fakt darmowych transakcji zdaje się to potwierdzać. Cały łańcuch operowany jest bezpośrednio przez Fundację NEO, także mogą sobie pozwolić na taki zabieg. W przypadku normalnej, nawet częściowo zdecentralizowanej kryptowaluty, byłoby to niemożliwe, gdyż sieć momentalnie zostałaby zainfekowana przez nieuczciwe jednostki.

Czołowi deweloperzy NEO, w publicznej rozmowie na platformie Github, w ramach rozmów na temat zmian w NEO 3.0 potwierdzają, że już teraz są organizacje, które bez żadnej bezpośredniej inicjatywy ekonomicznej płynącej z sieci (jak np. otrzymywanie opłat za weryfikowanie transakcji) są w stanie płacić za utrzymywanie Consensus Nodes. Krytyczna czerwona flaga dla projektu.



lerider commented on Jul 10, 2018 • edited ▾

A small increase in the supply of gas every year Reward consensus nodes

I strongly oppose these. The economic model is built upon circulation in a closed system, aligning interest so that both users and CN's have the same motives. Allowing increase in GAS based on for example reward to CN's nodes will create a system where CN's main interest is of economic gain and not for the benefit of users. It will result in a consortium of CN's who manipulate GAS price for their own maximized profit. It may potentially give a short term spike in NEO price when people are hoarding voting power (see EOS), but once hoarding is complete, the CN's will gain most benefit from "stabilizing" the consortium and we are stuck with CN's that never change owner (unless they dump on purpose). There are already dozens of parties who want to carry the cost of a CN (around 500 USD a month) without direct economic gain; I do not see a reason to overhaul the whole economic model.

Rysunek 10: Consensus Nodes bez wyraźnej inicjatywy ekonomicznej

³⁰ <https://blog.zerononsense.com/2018/10/04/neo-the-great-heist-an-analytical-research-case-study-pt-1-2/>

Blockchain nie może być zdecentralizowany, jeśli zarządzające nim węzły pilnujące konsensusu sieciowego, nie otrzymują nic w zamian. Oszukiwanie ekonomii nigdy nie wychodzi na dobre. W kryptowalutach, jest to możliwe jedynie w przypadku w pełni scentralizowanych blockchainów, kiedy to istnieje pośrednia inicjatywa finansowa. Przykład? Kiedy Fundacja NEO umawia się z daną firmą/grupą chętną do pokrycia kosztów utrzymania węzła, w zamian za np. możliwość zakupu udziałów w nowej spółce technologicznej powołanej przez NEO Global Capital. To tylko przykład i taka sytuacja (a przynajmniej nie przyznano tego nigdzie publicznie) nie miała miejsca. Pokazuje to jednak, że nie może istnieć zdecentralizowany system bez żadnego mechanizmu który wynagradzałby posiadaczy węzłów walidujących za ich usługę dla sieci.

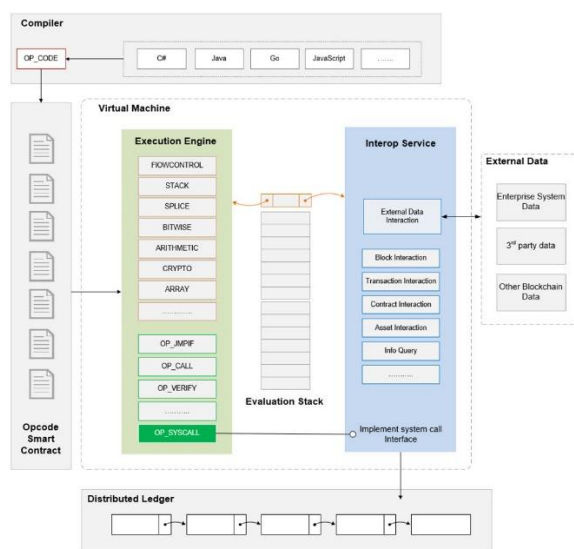
Smart Contracty

NEO, podobnie jak platformy takie jak Ethereum czy Waves, oferuje technologię smart contractów. Inteligentne kontrakty, są inteligentne jedynie z nazwy – jest to po prostu umowa napisana w kodzie, zamiast tradycyjnego pisma prawniczego, która możliwa jest do zrealizowania bez stron trzecich, automatycznie. Celem tego raportu nie jest zagłębianie się w technologię smart contractów, na temat której przeczytać możecie wiele opracowań w internecie. Pragnę jednak zwrócić uwagę, że NEO różni się od wymienionych platform elastycznością.

Smart contracty mogą być napisane w różnych środowiskach programistycznych³¹:

- C#, VB.Net, F#
- Java, Kotlin
- Python

Smart contracty są obecnie realizowane za pomocą NEO VM (Virtual Machine). Ma to ulec zmianie w NEO 3.0, jednak aktualny diagram przedstawiający konkretny cykl deponowania i realizacji kontraktu wygląda następująco:



Rysunek 11: Wirtualna Maszyna NEO

³¹ <https://docs.neo.org/en-us/sc/introduction.html>

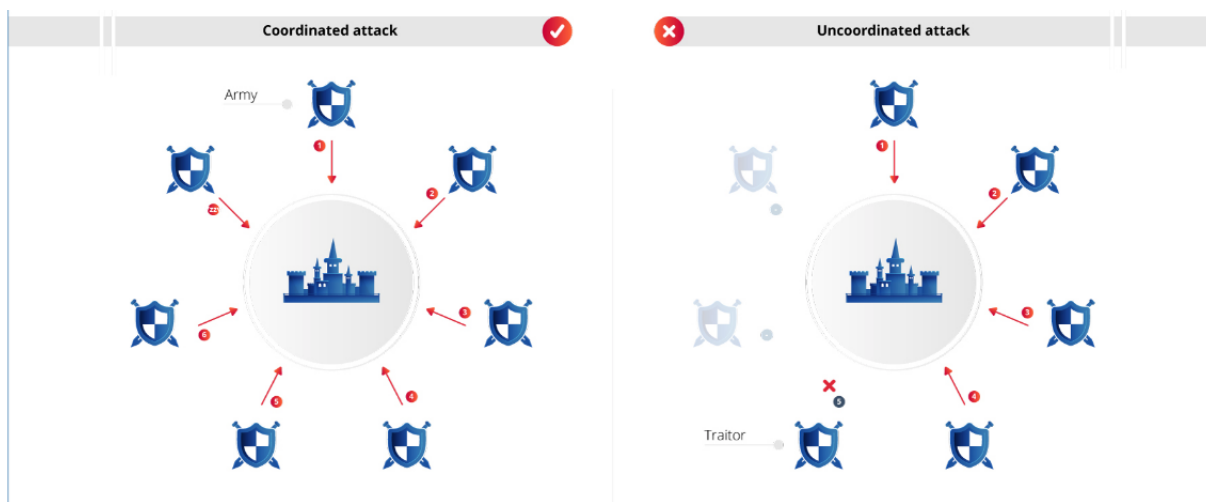
dBFT – Delegated Byzantine Fault Tolerance

Według słów Vitalika Buterina, twórcy Ethereum, panuje błędne przekonanie, jakoby protokoły konsensusu w kryptowalutach, miały uczynić je szybkimi. Prawda jest natomiast taka, że protokół konsensusu ma sprawić, że blockchain jest przede wszystkim bezpieczny.³² W takich słowach Vitalik skrytykował twierdzenia niektórych projektów, że dzięki użyciu dBFT mogą osiągnąć tysiące TPS (transakcji na sekundę). Owszem jest to możliwe, lecz takie kryptowaluty nie są zdecentralizowane – a przecież decentralizacja jest właśnie opus magnum kryptowalut. Twierdzenie te, było skierowane również w stronę NEO – które jak już ustaliliśmy posiada jedynie 7 węzłów walidujących, kontrolowanych w całości przez Fundację NEO. **Blockchain NEO ma zatem charakter prywatnego blockchainu, z możliwością publicznego wglądu do sieci.** Czym jednak jest ten cały dBFT?

dBFT to protokół konsensusu sieciowego blockchainu NEO. Cała otoczka wokół protokołów konsensusu (zgody) w zdecentralizowanych sieciach polega na jednym problemie: jak rozwiązać problem Generałów Bizantyjskich? ³³³⁴ Byzantine Fault Tolerance oznacza, że dwa węzły mogą bezpiecznie komunikować się przez sieć, wiedząc, że wyświetlają te same dane. Jest to kluczowe i jedno z najważniejszych zagadnień w kryptowalutach. Warto więc dowiedzieć się o nim nieco więcej.

Problem Generałów Bizantyjskich³⁵

Problem bizantyjskich generałów został pomyślany w 1982 r.³⁶ Jako dylemat logiczny ilustrujący, jak grupa bizantyjskich generałów może mieć problemy z komunikacją, próbując uzgodnić następny ruch w czasie ataku na przeciwnika.



Rysunek 12: Atak na wroga i Problem Bizantyjskich Generałów

Dylemat zakłada, że każdy z generałów dysponuje własną armią oraz, że każda z grup znajduje się w różnych miejscach miasta, które zamierzają zaatakować (jest zatem rozproszona). Generałowie muszą

³² <https://cryptoslate.com/analyzing-vitalik-buterins-statement-about-cryptos-centralized-piles-trash/>

³³ https://pl.wikipedia.org/wiki/Problem_bizantyjskich_genera%C5%82%C3%B3w

³⁴ <http://wazniak.mimuw.edu.pl/images/4/4a/Sr-11-wyk-1.0.pdf>

³⁵ <https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained>

³⁶ <https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf>

zgodzić się na atak lub wycofanie się. Nie ma znaczenia, czy atakują, czy wycofują się, dopóki wszyscy generałowie osiągną konsensus, tj. uzgodnią wspólną decyzję, wygrywają.

Dlatego możemy rozważyć następujące wymagania:

- Każdy generał musi zdecydować: zaatakować lub wycofać się (tak lub nie);
- Po podjęciu decyzji nie można jej zmienić;
- Wszyscy generałowie muszą uzgodnić tę samą decyzję i wykonać ją w sposób zsynchronizowany.

Wspomniane problemy komunikacyjne są związane z faktem, że jeden generał może komunikować się z innym tylko za pośrednictwem wiadomości, które są przekazywane przez kuriera. W związku z tym, głównym wyzwaniem problemu bizantyjskich generałów jest to, że wiadomości mogą zostać w jakiś sposób opóźnione, zniszczone lub utracone (a w najgorszym przypadku przechwycone przez wroga).

Ponadto, nawet jeśli wiadomość zostanie pomyślnie dostarczona, jeden lub więcej generałów może wybrać (z jakiegokolwiek powodu) złośliwe działanie i dopuścić się wysłania fałszywej wiadomości, aby wprowadzić w błąd innych generałów, co doprowadzi do całkowitej porażki.

Jeśli zastosujemy dylemat do kontekstu łańcucha bloków, każdy generał reprezentuje węzeł sieci. Węzły muszą osiągnąć konsensus w sprawie bieżącego stanu systemu. Innymi słowy, większość uczestników sieci rozproszonej musi się zgodzić i wykonać dokładnie to samo działanie, aby uniknąć całkowitej awarii.

Dlatego jedynym sposobem osiągnięcia konsensusu w tego typu systemach rozproszonych jest posiadanie przynajmniej większości niezawodnych i uczciwych węzłów sieciowych. Oznacza to, że jeśli większość sieci zdecyduje się działać złośliwie, system jest podatny na awarie i ataki. W praktyce, potrzebujesz więc większości wynoszącej min. 51% w węzłach uczciwych.

W kilku prostych słowach **bizantyjska odporność na błędy (BFT) jest własnością systemu, który jest w stanie oprzeć się klasie niepowodzeń wywodzących się z problemu bizantyjskich generałów**. Oznacza to, że system BFT może nadal działać, nawet jeśli niektóre węzły zawiodą lub działają złośliwie.

Istnieje więcej niż jedno możliwe rozwiązanie problemu bizantyjskich generałów, a zatem wiele sposobów budowania systemu BFT. Podobnie, istnieją różne podejścia do łańcucha bloków, aby osiągnąć bizantyjską odporność na błędy, a to prowadzi nas do tak zwanych algorytmów konsensusu.

NEO i konsensus sieciowy

W przypadku NEO, konsensus osiągany jest za pomocą protokołu dBFT – Delegated Bizantian Fault Tolerance, odmiany BFT dostosowanej do kryptowalut.

Zakładane 100 000TPS do 2020 roku w NEO to kolejny wymysł marketingowy który możemy wsadzić do kosza.³⁷ BFT jest stosowany w sieciach komputerowych od wieków³⁸, a konkretne badanie i ewaluacja protokołów konsensusu w kwestii kryptowalut i blockchainu, pokazuje jasno, że dBFT nie

³⁷ <http://www.lmdb.tech/bench/microbench/benchmark.html>

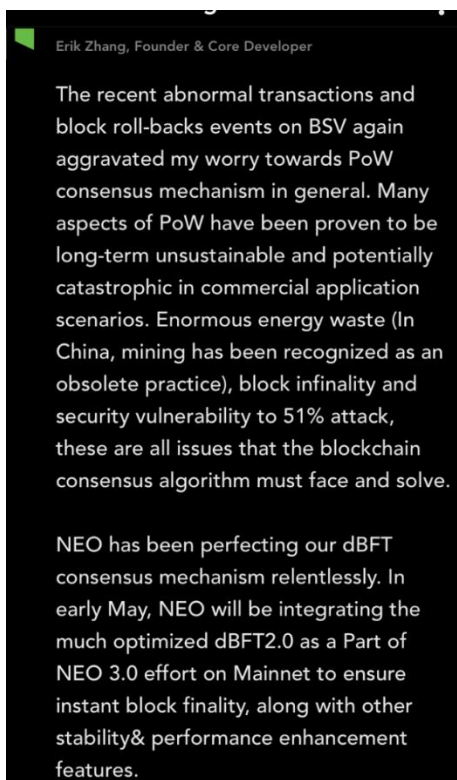
³⁸ <http://zoo.cs.yale.edu/classes/cs426/2012/bib/castro02practical.pdf>

może skalować się poza rozmiary małej, lokalnej i scentralizowanej sieci³⁹. Co więcej, niezwykle wątpliwe jest skalowanie takowego blockchainu do wielkości sieci Ethereum.

Jest to kolejne potwierdzenie, że NEO jest w rzeczywistości w pełni scentralizowane⁴⁰.

Bezpieczeństwo dBFT

Wątpliwe jest również wyższe bezpieczeństwo dBFT nad protokołem POW. Choć takie twierdzenia były robione przez Erika Zhanga:



Rysunek 13: Słowa Erika Zhanga nt. POW i dBFT

Jak pokazują dane z analizy przeprowadzonej przez centrum rozwoju NEO w Sant Petersburgu⁴¹, obrazujące dystrybucję zadań między węzłami walidującymi w obrębie blockchainu NEO, aby osiągnąć konsensus, wymagane jest min. 66,(6)% uczciwych węzłów. Zauważmy, że w przypadku POW i np. jego implementacji w Bitcoinie, aby główny łańcuch był zagrożony, atakujący musi dysponować 51% całkowitej mocy obliczeniowej.

Jeżeli więc 3 z 7 Consensus Nodes wykorzystywanych przez NEO zostanie z jakiegoś powodu uszkodzone, niesprawne, bądź zaatakowane, cały blockchain NEO przestaje działać, transakcje nie mogą być walidowane, a następne bloki tworzone. Może również dojść do rozłamu łańcucha. Stanowi to poważny problem, wręcz krytyczny, dla NEO, zważywszy również na fakt, że posiada jedynie 7

³⁹ <https://arxiv.org/pdf/1703.04057.pdf>

⁴⁰ <https://docs.neo.org/en-us/basic/consensus/whitepaper.html>

⁴¹ <https://medium.com/@neospcc/task-distribution-over-consensus-nodes-42f1349442ad>

węzłów walidujących (w dodatku wszystkie są scentralizowane, istnieje więc jeden punkt który wystarczy zaatakować, aby pogrążyć cały blockchain).

Jest to nie jedyny problem z jakim mierzy się NEO i jego blockchain. Jak sugeruje analiza kodu⁴², maksymalna ilość transakcji w bloku, jest ustalona na 500TPS, a nie zakładane i gorąco promowane w mediach społecznościowych 1000TPS.

Zastanawia również rodzaj użytych sygnatur kryptograficznych. Jest to ten sam multisig. znany z Bitcoina⁴³. Długi czas między blokami w Bitcoinie, zapewnia, że roczny wzrost wagi całego łańcucha bloków nie jest, aż tak znaczący. Natomiast zastosowanie tych samych sygnatur w przypadku blockchainu, którego czas bloków określony jest na 15s. (aktualizacja w NEO 3.0) powoduje, że rocznie łańcuch bloków zwiększa się o prawie 1GB (dokładnie - ponad 900MB). Powoduje to, że w przypadku wprowadzenia planowanego procesu decentralizacji, niezmiernie ciężko będzie utrzymywać, przez zwykłego użytkownika, kopię pełnego łańcucha. Prowadzi to do dalszej centralizacji sieci.

Opóźnienie i finalność w blockchainie

W celu lepszego zrozumienia proponowanych przez Erika Zhanga udoskonaleń w protokole dBFT 2.0, myślę, że należyte byłoby pewne wprowadzenie, czym są i jaką funkcję odgrywają w kryptowalutach opóźnienie i finalność (ang. Latency & Finality). Ponieważ właśnie opóźnienie i finalność ma zostać poważnie usprawnione w dBFT 2.0⁴⁴.

Opóźnienie - czas, jaki upływa od utworzenia transakcji do momentu potwierdzenia jej przyjęcia przez blockchain (i jak pewność jej akceptacji wzrasta z upływem czasu).

Finalność - właściwość, że po zakończeniu transakcji nie ma możliwości jej odwrócenia (lub zmiany). Zasadniczo jest to moment, w którym strony biorące udział w transferze mogą uznać zawartą umowę (w tym wypadku transakcję) za finalną i nieodwracalną. Finalność może być deterministyczna lub probabilistyczna.

Obie z tych cech odgrywają kluczową rolę w przypadku blockchainu⁴⁶. To od nich zależy, jak szybko nasza transakcja znajdzie się w sieci oraz czy możemy uznać ją za bezpieczną. Docelowo, jeżeli chcemy skalować nasz system do globalnych rozmiarów, a także wykorzystywać go jako np. błyskawiczny system rozliczeniowy, opóźnienie musi być jak najmniejsze (najlepiej nie większe niż kilka sekund), a finalność powinna:

- dążyć do wartości 1
- osiągać wartość 1 (maksimum – pewność, że nasza transakcja jest w głównym łańcuchu, jest bezpieczna i nieodwracalna)

Może to brzmieć zaskakująco, ale większość blockchainów, w tym Bitcoin, nie posiada deterministycznej ostateczności. Dla każdego danego bloku istnieje jedynie teoretyczna (zakładana

⁴² <https://blog.zerononsense.com/2018/08/31/serious-issues-with-neo-it-does-not-work/>

⁴³ <https://en.bitcoin.it/wiki/Multisignature>

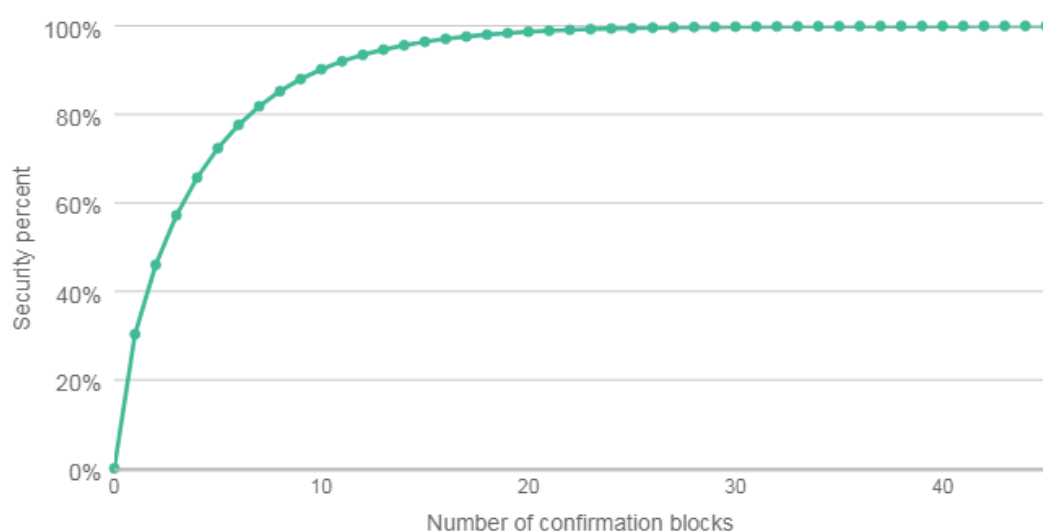
⁴⁴ <https://unhashed.com/cryptocurrency-news/neo-releases-dbft-2-0-for-better-transaction-finality/>

⁴⁵ https://docs.neo.org/en-us/08_dbft.pdf

⁴⁶ <https://hackernoon.com/latency-and-finality-in-different-cryptocurrencies-a7182a06d07a>

przez użytkowników) możliwość, że dłuższy łańcuch, będzie propagowany przez sieć. Ponieważ protokół nakazuje, aby węzły zawsze akceptowały najdłuższy łańcuch jako ważny, oznacza to, że wszystkie bloki z początkowego łańcucha, które nie są częścią drugiego, dłuższego łańcucha, zostaną odrzucone. Dlatego ostateczność w przypadku Bitcoina jest probabilistyczna, a więc wzrasta z czasem. Mówiąc po ludzku – im więcej mamy potwierdzeń z sieci, tym nasza transakcja staje się bezpieczniejsza i pewniejsza. Maleje tym samym prawdopodobieństwo jej odwrócenia przez atakującego.

Nieodwracalność transakcji i jej bezpieczeństwo stanowią podstawę i największy atut łańcucha bloków. Dlatego skuteczna optymalizacja tych parametrów, stanowi podstawę w udoskonalaniu takiego systemu. Zwyczajowo zakłada się, że w momencie zatwierdzenia transakcji na łańcuchu głównym, staje się ona całkowicie bezpieczna. Spójrzmy więc jak rozkłada się prawdopodobieństwo odwrócenia transakcji przez osobę bądź podmiot dysponujący znaczną mocą obliczeniową zasilającą dany łańcuch bloków, który przeprowadza atak na łańcuch główny. Jak bezpieczne są twoje transakcje?



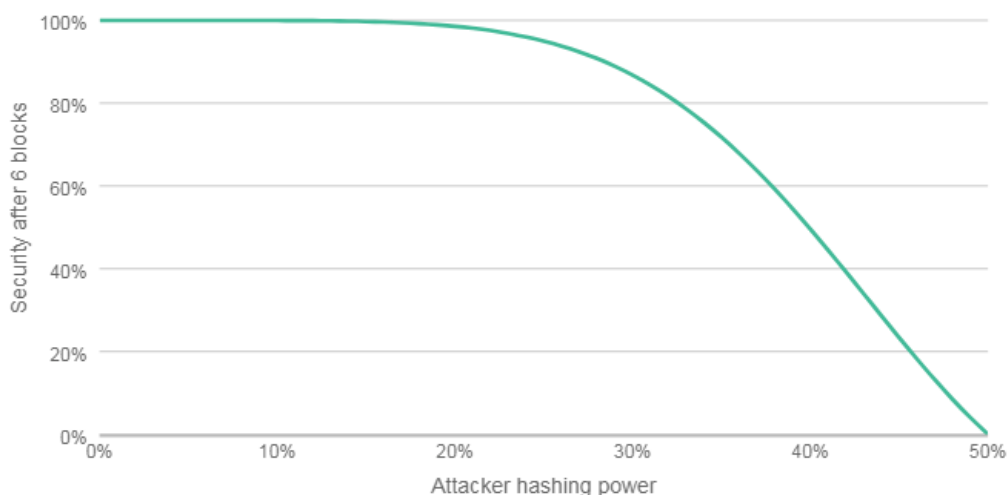
Rysunek 14: Rozkład bezpieczeństwa transakcji w zależności od potwierdzeń z sieci

Diagram stworzony został na podstawie oryginalnego kodu z Whitepaper Bitcoina⁴⁷. Oto jak bezpieczna jest nasza transakcja w zależności od ilości potwierdzeń z sieci:

- 30.3% bezpieczeństwa po 1 potwierdzeniu
- 77.6% bezpieczeństwa po 6 potwierdzeniach
- 90.2% bezpieczeństwa po 10 potwierdzeniach
- 99.99% bezpieczeństwa po 45 potwierdzeniach

Biorąc pod uwagę częste założenie, że 6 transakcji jest wystarczające (ok. 1h w przypadku Bitcoina) dla pełnego bezpieczeństwa sieci, spójrzmy jak oto kilka liczb, które pokazują poziom bezpieczeństwa w zależności od procentu mocy obliczeniowej kontrolowanej przez atakującego, gdy transakcja zostanie zatwierdzona w 6 blokach uczciwego łańcucha:

⁴⁷ <https://bitcoin.org/bitcoin.pdf>



Rysunek 15: Rozkład bezpieczeństwa transakcji po 6 blokach w zależności od poziomu mocy obliczeniowej posiadanej przez atakującego

- 99.99% bezpieczeństwa transakcji, jeżeli atakujący posiada 8% mocy obliczeniowej
- 95% bezpieczeństwa transakcji, jeżeli atakujący posiada 25% mocy obliczeniowej
- 78.68% bezpieczeństwa transakcji, jeżeli atakujący posiada 33% mocy obliczeniowej
- 49.6% bezpieczeństwa transakcji, jeżeli atakujący posiada 40% mocy obliczeniowej
- 4.06% bezpieczeństwa transakcji, jeżeli atakujący posiada 49% mocy obliczeniowej

Jak więc można wywnioskować, optymalizacja opóźnień (ang. latency) i finalności (ang. finality) to klucz do wielkoskalowych, szybkich i bezpiecznych łańcuchów bloków. Różne kryptowaluty⁴⁸ proponowały różne rozwiązania tego problemu. Jak zapewnić, aby transakcja transmitowana była do sieci w minimalnym opóźnieniu, jednocześnie stawiała się bezpieczna po jak najmniejszej ilości potwierdzeń z sieci i wydobytych bloków. Kryptowaluta Stellar Lumen, zamiast posiadać pewną liczbę niepotwierdzonych transakcji (tzw. pool) tak jak to ma miejsce w przypadku Bitcoina, każdy z węzłów walidujących zatwierdza samodzielnie, czy dana transakcja jest poprawna. Dopiero wtedy komunikuje się z resztą węzłów i potwierdza transakcję.

Problem ciągłego komunikowania się ze wszystkimi węzłami na raz może zagrozić skalowaniu się Stellar, jednak zostało to rozwiązane za pomocą wprowadzenia tzw. zaufanej grupy węzłów lokalnych. Chodzi o to, że każdy z węzłów posiada kilka z zaufanych bliźniaczych węzłów, które potwierdzają transakcję, po tym gdy zostanie ona uznana za poprawną. Niepotrzebne jest więc komunikowanie się ze wszystkimi węzłami, gdyż tworzą nam się „lokalne obszary zaufanych węzłów”, na których opiera się sieć i którym można zaufać. Co prawda, blockchain kryptowaluty Stellar zarządzany jest obecnie przez jedynie 65 węzłów walidujących⁴⁹, nie wiemy więc, jak ten system sprawdzałby się w skali np. Bitcoina.

W celu optymalizacji finalności i opóźnień, kryptowaluty takie jak IOTA czy NANO poszły o krok dalej. IOTA wykorzystuje do tego zupełnie nowy rodzaj protokołu: ang. Tangle.⁵⁰ Jednak w przypadku obu z nich, istnieją poważne problemy wiążące się z rzeczywistą decentralizacją. IOTA do działania

⁴⁸ <https://hackernoon.com/latency-and-finality-in-different-cryptocurrencies-a7182a06d07a>

⁴⁹ <https://stellarbeat.io/>

⁵⁰ <https://www.iota.org/research/meet-the-tangle>

potrzebuje pojedynczego węzła znanego koordynatorem, zarządzanego przez Fundację IOTA. Nie można więc uczciwie mówić o jakiegokolwiek decentralizacji sieci, jeśli jej funkcjonowanie opiera się na pojedynczym punkcie awarii (ang. single point of failure). Jak więc możecie zauważyć, udoskonalanie tych dwóch atrybutów w blockchainie jest niezwykle kłopotliwe i zwyczajnie skomplikowane technicznie.

Zmiany w protokole dBFT 2.0⁵¹ odnośnie finalności są następujące: pojedyncza transakcja nie musi być zatwierdzana przez wszystkie węzły, a raczej przez konkretną minimalną ich ilość. Opisuje to równanie:

$$M = 2f + 1$$

$$f = 1/3 \times N$$

M – minimalna ilość wymaganych podpisów autentyczności od węzłów

N – ilość węzłów walidujących (Consensus Nodes) w sieci

Krótkie obliczenia: NEO posiada obecnie 7 CN (Consensus Nodes). Zatem, aby zatwierdzić transakcję, potrzebne jest potwierdzenie z:

$$f = 1/3 \times 7 \rightarrow f = 7/3$$

$$M = 2 \times 7/3 + 1 = \sim 6 \text{ węzłów}$$

Zatem, w nowym protokole dBFT 2.0 wymagane będzie jedynie 6 węzłów do zatwierdzenia transakcji (o ile liczba CN nie ulegnie zmianie). Sprawi to, że rozkład finalności, w wykładniczym diagramie, gdzie OX oznacza liczbę bloków, a OY poziom bezpieczeństwa (nieodwracalności transakcji) przyjmie kształt funkcji wykładniczej. Konkretnie dane nie są na tą chwilę dostępne, gdyż protokół nie został jeszcze wprowadzony do systemu NEO. Twierdzenie Erika Zhanga, że dzięki dBFT 2.0 finalność osiągnie wartość maksymalną = 1 (czyli pewność, że transakcja jest bezpieczna na głównym łańcuchu i nie może zostać odwrócona) można włożyć między bajki.^{52 53}

Natomiast w kwestii finalności, brakuje konkretnych danych technicznych opisujących jak proponuje się udoskonalenie tej cechy. Niemniej, jak pokazuje przykład kryptowaluty Stellar, w przypadku mniej zdecentralizowanych sieci (a udowodniliśmy już, że NEO jest w pełni scentralizowane) zmniejszenie opóźnienia nie powinno być wielkim problemem, gdyż nie trzeba martwić się poziomem decentralizacji sieci.

“(...) wiemy, że system nie wykorzystuje żadnych ekonomicznych inicjatyw i wymaga ogromnego zaufania, co jest po prostu niedopuszczalne w kryptowalutach” – Eric Wal, krytyka dBFT w NEO

⁵¹ https://docs.neo.org/en-us/08_dbft.pdf

⁵²

https://twitter.com/neoerikzhang/status/1080712557650825216?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweteembed%7Ctwterm%5E1080712557650825216&ref_url=https%3A%2F%2Funhashed.com%2Fcryptocurrency-news%2Fneo-releases-dbft-2-0-for-better-transaction-finality%2F

⁵³ <https://unhashed.com/cryptocurrency-news/neo-releases-dbft-2-0-for-better-transaction-finality/>

Tokenekonomia – NEO i GAS

Wprowadzenie do modelu dwutokenowego

Być może znacie ten model. Jeden projekt, ale dwie kryptowaluty. To tak jak mężczyzna i dwie kobiety – bardzo rzadko działa. Nie inaczej jest w przypadku kryptowalut. Kiedy projekt decyduje się na własną kryptowalutę, już w takim momencie staje przez potwornie trudnym zadaniem. Jak zapewnić wartość i użyteczność nowo powstałej kryptowaluty. Dlatego, skutecznym rozwiązaniem jest zazwyczaj wykorzystanie już istniejących – w szczególności budowa swojego biznesu wokół sprawdzonych i zaufanych (oraz popularnych) systemów: Bitcoina, Ethereum.

Niemniej, model dwutokenowy, choć kuszący dla spekulantów i małych inwestorów, mogący sprawić na giełdzie nieco zamieszania i wzrostów, długofalowo stanowi duże zagrożenie dla funkcjonowania i rozwijania się projektu. Ciężko dziś znaleźć zastosowanie dla jednej nowej kryptowaluty (o ile nie jest tak rewolucyjna jak np. Ethereum i wprowadzona w nim technologia inteligentnych kontraktów), a co dopiero stworzyć świetnie (albo przynajmniej dobrze) funkcjonujący ekosystem, w którym wykorzystywane są dwa odrębne tokeny, bądź kryptowaluty. Warto zauważyć, że nie tylko NEO posiada w swoim arsenale dwie kryptowaluty. Podobny model (prawie taki sam) wykorzystuje chociażby Vechain Thor⁵⁴ i Tefood⁵⁵⁵⁶.

NEO

NEO⁵⁷ to jeden z tokenów w modelu dwutokenowym. Jego maksymalna podaż do 100M, jest niepodzielne (minimalnie możesz wysłać 1NEO), a według Whitepaper⁵⁸ i pierwotnych założeń, token miał działać podobnie do standardowej akcji firmy notowanej publicznie – stanowić prawo głosu w systemie NEO. Dzięki NEO (tokenowi) moglibyśmy głosować na kandydatów na węzły walidujące. Nie zostało to jednak dotychczas wprowadzone. Należy również zauważyć, że NEO, inaczej niż tradycyjna akcja, nie daje ci żadnego udziału w Fundacji NEO. Jakie są zatem funkcjonalności NEO na tą chwilę?

Może je wysyłać, odbierać oraz przechowywać w portfelu, dzięki czemu generują GAS. Nic więcej. Czyni to samo NEO, w mojej definicji, aktywem cyfrowym. Gdyż nie posiada cech kryptowaluty – nie możemy dokonywać płatności, nie jest również zdecentralizowane, w dodatku jest niepodzielne, nie ma więc standardowej i wymaganej funkcji pieniądza. Planowane funkcję głosowania również nie zostały zaimplementowane, zatem nie można o NEO mówić jako o tokenie (gdyż token posiada funkcję w ekosystemie). NEO można by nazwać tokenem w momencie, kiedy to GAS miałby, planowane od dawna, cechy. Jednak i on, jest na tą chwilę, w większości bezużyteczny.

⁵⁴ <https://vechaininsider.com/guides/guide-to-vechain-nodes-and-node-rewards/>

⁵⁵ <https://medium.com/te-food/token-economy-of-te-food-b617efe17115>

⁵⁶ <https://medium.com/te-food/token-economics-of-calories-cal-8ce9eb301091>

⁵⁷ <https://crushcrypto.com/neo-cryptocurrency-deep-dive/>

⁵⁸ <https://docs.neo.org/en-us/whitepaper.html>

NEO notowane jest na większości giełd kryptowalut: Binance, Bitfinex (gdzie możemy handlować NEO na tzw. margin), czy Bittrex.

Market Cap ⓘ	\$0.69B
Market Cap Y2050 ⓘ	\$1.07B
Reported 24Hr Volume	\$0.26B
24Hr Price Change	-1.32%
Reported Supply	65,000,000.00
Y2050 Supply ⓘ	100,000,000.00
% Y2050 Supply Issued ⓘ	65.00%
All Time High (01/15/2018)	\$194.79
% down from ATH	-94.51%

Rysunek 16: NEO Market Cap

Pomimo braku jakichkolwiek funkcji, NEO okazało się być jednym z najlepszych aktywów cyfrowych w jakie tylko można było zainwestować. Fascynacja inwestorów Chińskimi projektami w czasie hossy z 2017 roku, a także przydomek „Ethereum Chin” i szukanie kolejnych inwestycji mogących zapewnić zwroty porównywalne z tymi z Ethereum (kiedy to wycena giełdowa wzrosła z \$0.3 USD do ponad \$1200 USD), sprawiły, że rzeczywiście, NEO wzrosło o nieprawdopodobny procent wartości. Pokazuje to następujące zestawienie:

Historical ROI	
1 week	-3.36%
1 month	+16.11%
3 months	+42.68%
1 year	-85.74%
2 years	+5947.31%
Supply Snapshot	
Type	Fixed
Max	100000000
Ongoing emission type	N/A

Rysunek 17: NEO ROI

Jak można zauważyć, brak jakiejkolwiek użyteczności i dobry marketing czynią cuda w świecie kryptowalut. Warto nadmienić, że jeśli umieścimy NEO na dedykowanym portfelu od twórców (Neon,

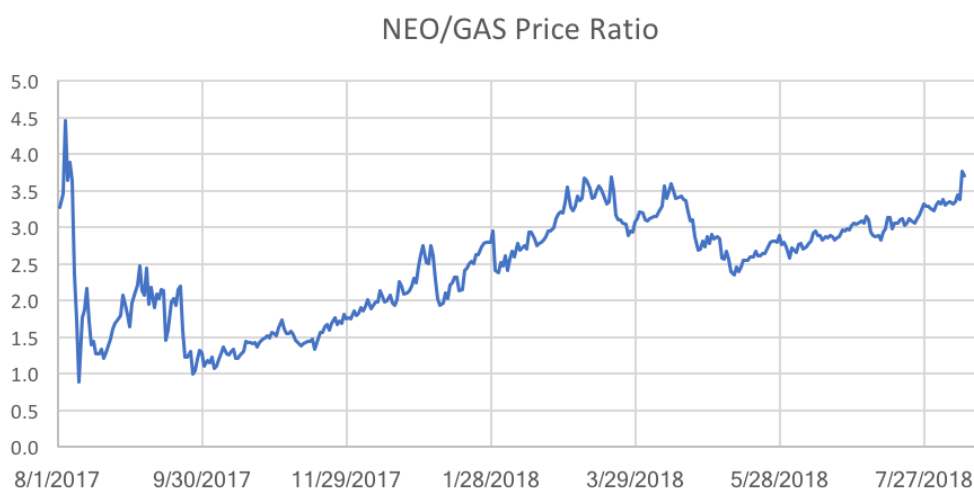
NEO GUI) lub na giełdzie Binance lub Kucoin, generuje ono GAS. Jedno NEO generuje 1GAS w ciągu 22 lat. Poniżej znajdziecie wykres zakładanej emisji GAS w oparciu o dostępne dane.

GAS

GAS miał być, jak sama nazwa mówi, paliwem napędzającym blockchain NEO. To właśnie za jego pomocą płacilibyśmy transakcje w sieci NEO, to on potrzebny byłby do deponowania smart contractów, to on stałby się fundamentem Smart Economy. Cóż takie było założenie. Natomiast jedyną własność GASu która rzeczywiście działa to płacenie za deponowanie inteligentnych umów w sieci NEO – potrzebujemy do tego 500 jednostek GAS. Wysoki koszt smart contractów i niska emisja GAS sprawiają, że deweloperzy z ramienia Fundacji NEO posiadają ścisłą kontrolę na deponowanymi w sieci smart contractami.

Transakcje w sieci NEO są darmowe⁵⁹. Jak więc możecie zauważyć, nie istnieje żadna inicjatywa ekonomiczna dla węzłów walidujących. Z założenia miały one otrzymywać tzw. transaction fees – czyli opłaty za walidowanie transakcji, które użytkownicy sieci płaciliby właśnie w GAS. Obecnie jednak taki model nie został przyjęty i pozostaje on w sferze planów. Co więcej, być może ulegnie on zmianie wraz z trwającą dyskusją na temat NEO 3.0 pomiędzy deweloperami na Githubie.

Wiele wyliczeń pokazuje również, że GAS w stosunku do NEO jest mocno niedowartościowany^{60,61}. Być może wynika to ze złego pojmowania inwestorów czym rzeczywiście jest GAS, a czym NEO i jakie role odgrywają w systemie. To właśnie GAS powinien mieć (jeżeli podążałoby się ściśle według założeń deweloperów budujących blockchain NEO) największą wartość, ze względu na swoją niską emisję i użyteczność. Jednak jak to mówią, rynek nigdy się nie myli – możliwe, że funkcje NEO i GAS zostały źle zakomunikowane do społeczności, albo sam system nie sprawdza się jak powinien wychodząc z założeń. Niemniej, jest to ciekawa sytuacja.



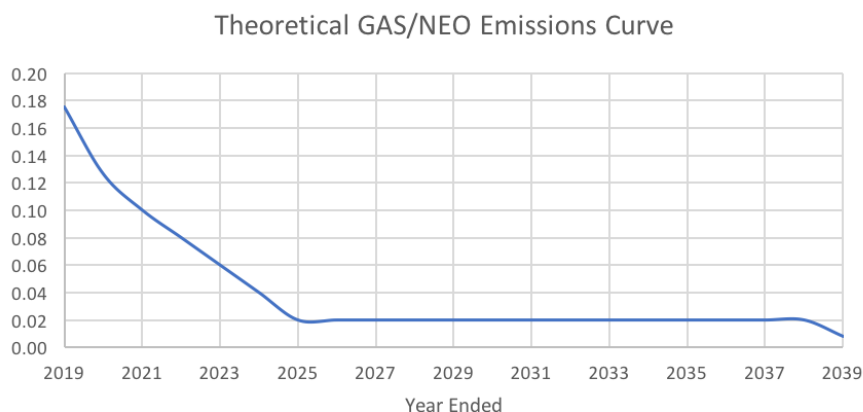
Rysunek 18: NEO/GAS stosunek cenowy na przestrzeni roku

⁵⁹ <https://docs.neo.org/en-us/sc/systemfees.html>

⁶⁰ <https://medium.com/@emil.sandstedt/neo-and-gas-exploring-the-price-difference-a47029ff215a>

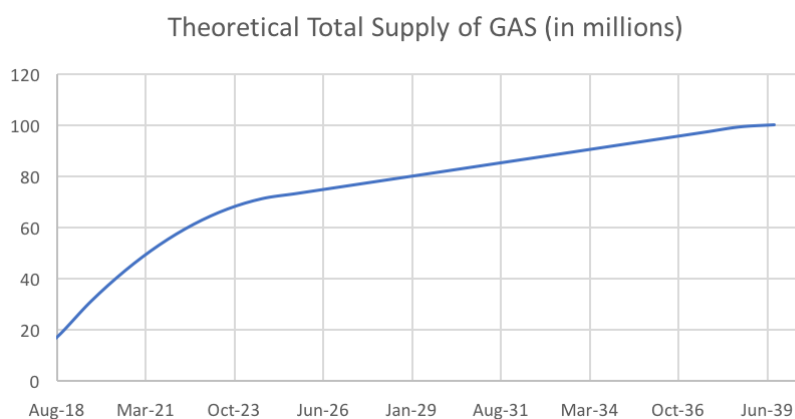
⁶¹ <https://lucylabs.io/neo-is-overvalued-versus-gas/>

Model emisji GAS w stosunku do podaży rynkowej NEO:



Rysunek 19: NEO i GAS, teoretyczna krzywa emisyjna

Zakładamy (jeżeli zasady funkcjonowania sieci nie ulegną zmianie i nie zostanie wprowadzona np. inflacja GAS) model całkowitej podaży GAS w czasie:



Rysunek 20: GAS - podaż na linii czasu

Zmiany w modelu NEO i GAS

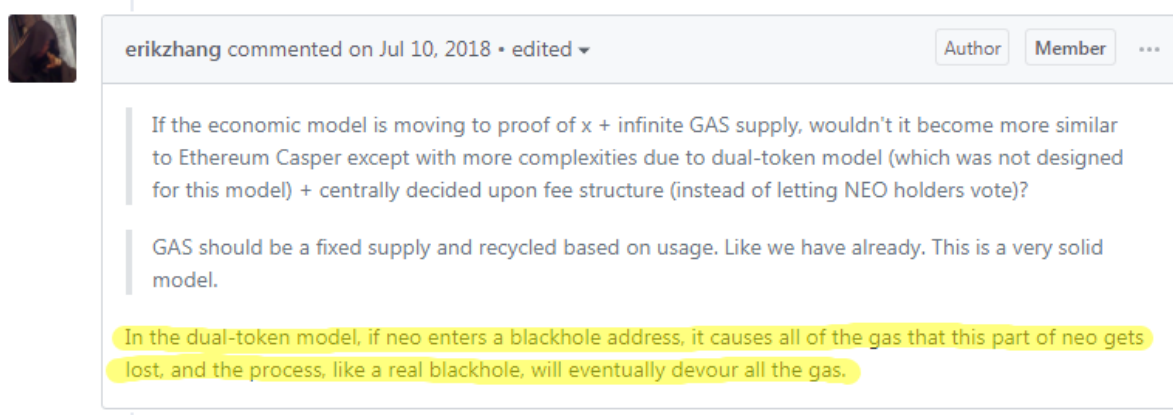
Planowane NEO 3.0 ma również wnieść sporo zmian do modelu NEO i GAS. Wynikają one z kilku niebezpiecznych problemów technicznych odnalezionych przez deweloperów w systemie, a także czynników ekonomicznych. W tej sekcji, przyjrzymy im się bliżej. Wszystkie z zaprezentowanych niżej zrzutów ekranu pochodzą z oficjalnych dyskusji nt. NEO 3.0 na otwartej platformie Github⁶².

Pierwszym z problemów technicznych są tzw. adresy „blackhole”. Czarne dziury w sieciach komputerowych oznaczają miejsca w których ruch sieciowy jest przerywany, jednak bez informowania o tym źródła⁶³. Przykładem czarnych dziur mogą być np. adresy e-mail, służące do wysyłanie jednorazowych wiadomości email. Jeżeli próbujemy odpowiedzieć na wiadomość, zostaje ona automatycznie usunięta i nigdy nie trafia do adresata.

⁶² <https://github.com/neo-project>

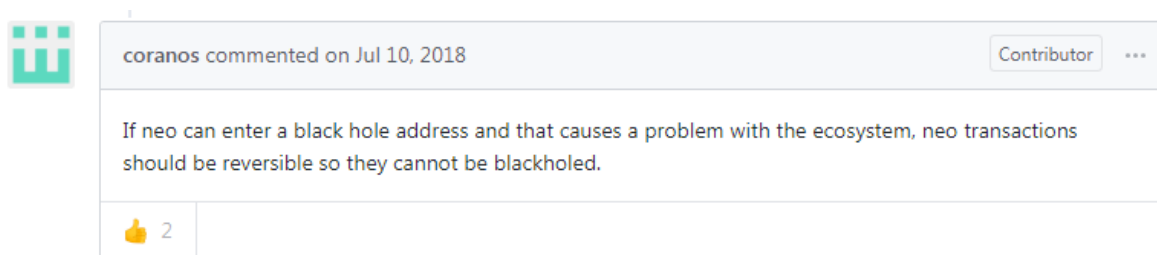
⁶³ [https://pl.wikipedia.org/wiki/Czarna_dziura_\(sieci_komputerowe\)](https://pl.wikipedia.org/wiki/Czarna_dziura_(sieci_komputerowe))

Przypomnijmy – Erik Zhang jest współzałożycielem i głównym architektem blockchainu i całego ekosystemu NEO.



Rysunek 21: Erik Zhang - Github: problem "czarnych dziur" w NEO

W powyższym, rozważane było wprowadzenie czynnika inflacyjnego w GAS. Oznaczałoby to, że GAS nie posiadałby już określonej, ustalonej ilości (odpowiadającej 100M NEO, przy czym każde wytworzy 1GAS w ciągu 22lat). Zamiast tego GAS poddany byłby inflacji, stosunkowo małej, jednak byłaby to niezwykle istotna, fundamentalna zmiana (do której Fundacja NEO ma pełne prawo, gdyż kontroluje całą sieć – dotknięci mogą się jednak poczuć inwestorzy). Inflacja, miałaby spowodować, że NEO wpadające w „czarną dziurę” nie spowoduje reakcji łańcuchowej, w której w krótkim czasie, cały GAS zostałby pochłonięty.



Rysunek 22: Pomysł na możliwość odwrócenia transakcji w NEO

Jedną z największych, jeśli nie największą zaletą kryptowalut jest to, że odmiennie aniżeli w przypadku tradycyjnego świata finansów, raz dokonana transakcja nie może być przez nikogo zablokowana, cofnięta (jeżeli nie dojdzie do zmasowanego ataku na sieć, jak opisałem wyżej), odwrócona. Wyślesz kryptowalutę – np. do swojej rodziny w Australii – żaden organ rządowy nie jest w stanie tej transakcji odwrócić i skonfiskować twoich monet.

Tym bardziej zastanawiająca jest propozycja rozwiązania problemu czarnych dziur w sieci NEO za pomocą możliwości odwracania transakcji (gdyby jakieś NEO wpadło w martwy adres). Co prawda, niektóre scentralizowane kryptowaluty (które nie powinny z powodu centralizacji w ogóle być nazywane kryptowalutami), takie jak EOS, posiadają możliwość cofnięcia transakcji⁶⁴. Jest to jednak krytyczna czerwona flaga, która powinna odstraszać cię od danego projektu, gdyż oznacza ona, że twoje fundusze nie są bezpieczne. Na razie w przypadku NEO, cofanie transakcji pozostaje w fazie

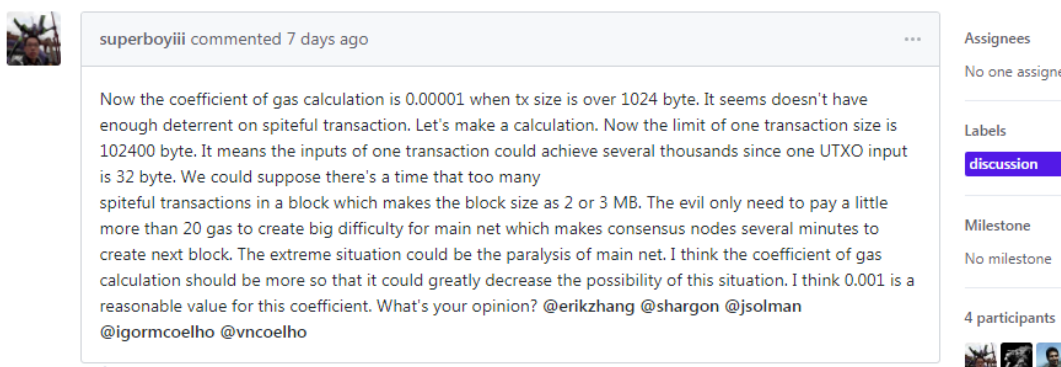
⁶⁴[https://cointelegraph.com/news/eos-reverses-previously-confirmed-transactions-as-pundits-decry-
centralization](https://cointelegraph.com/news/eos-reverses-previously-confirmed-transactions-as-pundits-decry-centralization)

pomysłów, jednak sama taka propozycja od czołowych deweloperów, jest aktem czystej ignorancji i niezrozumienia czym rzeczywiście kryptowaluty są i do jakich celów powinny służyć.

Pojawiły się również informacje o krytycznym błędzie w kodzie NEO⁶⁵, prowadzący do kompletnego paraliżu sieci, bądź – w najlepszym wypadku, opóźnienia w wydobywaniu bloków o kilka minut.

Increase the coefficient of gas calculation to 0.001 when tx size is over 1024 byte #708

Open superboyiii opened this issue 7 days ago · 4 comments



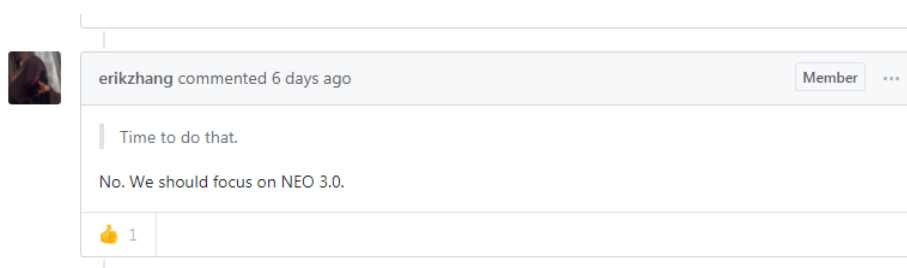
superboyiii commented 7 days ago

Now the coefficient of gas calculation is 0.00001 when tx size is over 1024 byte. It seems doesn't have enough deterrent on spiteful transaction. Let's make a calculation. Now the limit of one transaction size is 102400 byte. It means the inputs of one transaction could achieve several thousands since one UTXO input is 32 byte. We could suppose there's a time that too many spiteful transactions in a block which makes the block size as 2 or 3 MB. The evil only need to pay a little more than 20 gas to create big difficulty for main net which makes consensus nodes several minutes to create next block. The extreme situation could be the paralysis of main net. I think the coefficient of gas calculation should be more so that it could greatly decrease the possibility of this situation. I think 0.001 is a reasonable value for this coefficient. What's your opinion? @erikzhang @shargon @jsolman @igormcoelho @vncoelho

Assignees: No one assigned
Labels: discussion
Milestone: No milestone
4 participants

Rysunek 23: źródło: Github - krytyczny błąd w GAS

W tak poważnym błędzie wysoce zastanawiające jest stanowisko Erica Zhanga, który całą sytuację skomentował, że powinni skupić się na NEO 3.0:



erikzhang commented 6 days ago Member

Time to do that.

No. We should focus on NEO 3.0.

1

Rysunek 24: Odpowiedź Erica Zhanga - głównego architekta blockchainu NEO

Ostatnią alarmującą rzeczą jaką udało mi się w propozycji zmian w NEO 3.0 znaleźć, jest skupienie się na promowaniu funkcjonalności systemu bezpośrednio związanych z możliwą wyceną giełdową. Nie jest przesadą mówić, że akurat spekulacja powinna być ostatnią rzeczą na którą zwracamy uwagę w momencie projektowania sprawnego i zdecentralizowanego systemu. NEO wnosi, że jest projektem open-source, a Fundacja NEO organizacją non-profit. Takie twierdzenia niestety poddają te informacje w wątpliwość.

⁶⁵ <https://github.com/neo-project/neo/issues/708>

Make neo divisible

The only thing this would help is to allow distribution of smaller GAS fees. The small benefit does not justify the big risk forced upon token holders.

1. NEO is the governance token and GAS is the utility token. The characteristics of the tokens support this; if you want to fuel a contract with a system asset, then you use the utility token (GAS). This will increase demand on GAS token as the network usage increases, and in turn increase value of NEO when GAS is recycled. **Allowing NEO to be divisible create a big risk that dApps choose to fuel themselves with NEO token instead. This may be negative in terms of token price for both NEO and GAS token; as GAS loses demand, the value decrease. As the recycling benefit decreases in value, NEO token may also lose value.** This is my personal expectation, and I do not see the big risk for token holders justify the small benefit.
2. Even though high voting participation is beneficial, we would like to avoid random voting as much as possible. Allowing fractional NEO to vote (for reward) will give much power to wallet creators, as they will certainly implement a "vote standard" function (for their own nodes?) to make it easier to vote for users. People who are more invested will have more incentive to vote "properly", and keeping the NEO as indivisible is at least a small barrier for participation in voting (for good and bad).

Rysunek 25: NEO i dyskusja o cenie

Portfele NEO

Jeżeli chodzi o składowanie swoich NEO – chcesz robić to na portfelu do którego klucze prywatne posiadasz! Tylko wtedy, kryptowaluty są prawdziwie twoje!

Polecam dwa portfele: NEON Wallet⁶⁶ oraz NEO GUI⁶⁷. Ten pierwszy jest preferowany jeśli jesteś mało doświadczony w kryptowalutach, bądź preferujesz dobry design i UI, natomiast NEO GUI – czyli po prostu graficzna implementacja interfejsu użytkownika, oferuje bogatą liczbę funkcji. Powinieneś go wybrać, jeśli zainteresowany jesteś budowaniem na NEO jako deweloper.

Tokeny na NEO – NEP5 standard

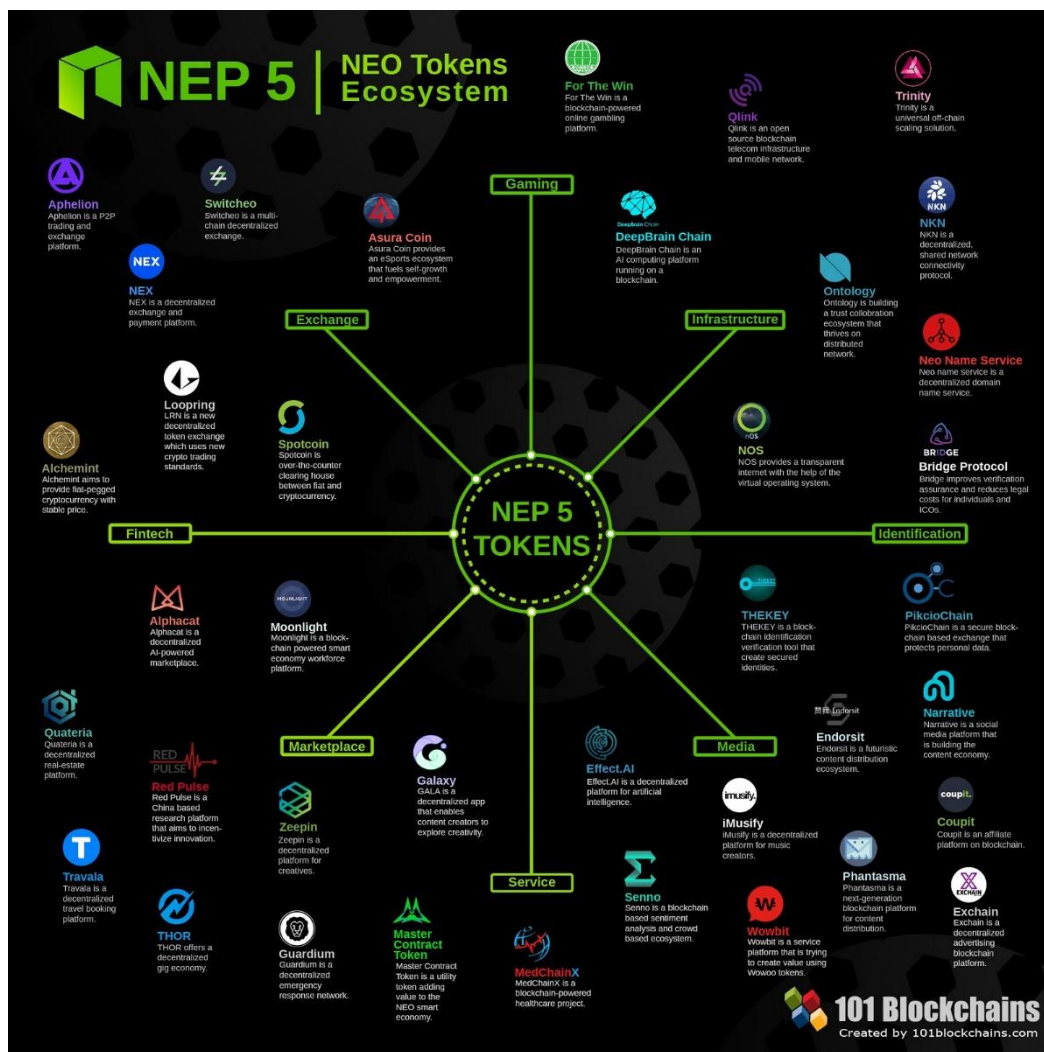
Obecnie na NEO istnieją 54 działające i sprawne projekty, posiadające swój token w standardzie NEP5. Nie różni się on wiele od znanego nam z Ethereum ERC20. Co więcej, to właśnie ERC20⁶⁸ stanowił dobrą podpowiedź dla deweloperów w czasie tworzenia NEP5. Szlaki były już przetarte, wystarczyło dostosować kod do multiplatformowości oferowanej przez NEO. Tak więc, NEP5 jest zwyczajnie odpowiednikiem ERC20.

Wszystkie projekty które przeprowadziły ICO na platformie NEO, są obecnie w standardzie NEP5. Całość prezentuje poniższa grafika:

⁶⁶ <https://neonwallet.com/>

⁶⁷ <https://github.com/neo-project/neo-gui/releases>

⁶⁸ <https://hackernoon.com/nep-5-neos-answer-to-ethereum-erc-20-tokens-69d9b082c9e1>



Rysunek 26: Tokeny w standardzie NEP5 – źródło: 101 Blockchains

Grafika jest nieco przestarzała, gdyż np. projekt Thor, zakończył niedawno swoją działalność, pozostawiając inwestorów na lodzie⁶⁹. Reszta danych się zgadza. Jednak sytuacja z Thor jasno pokazuje, jak ważna jest dokładna analiza kryptowalut oraz prawidłowa dywersyfikacja i przysłowiowe, nie wkładanie wszystkich naszych jajek do jednego koszyka. Jeden konkretny altcoin, o ile nie znajduje się na wysokiej pozycji w rankingu kryptowalut, nie powinien stanowić więcej niż 3-5% waszego ogólnego portfolio. Wynika to właśnie z obawy przed możliwym zamknięciem projektu, kiedy to inwestor pozostaje bez jakichkolwiek środków, które w dany projekt zainwestował.

Tokeny w standardzie NEP5 możecie składać dokładnie w takim samym sposób jak robi się to z NEO i GAS. Zarówno NEON Wallet i NEO GUI będą do tego odpowiednie. Przepływ transakcji tokenami, możecie śledzić za pomocą NeoTracker⁷⁰.

Jedynie część z tokenów NEP5 dostępna jest na największych giełdach światowych – głównie Binance. Jednak wszystkie z nich możecie spokojnie wymieniać na Switcheroo⁷¹. Uważaj jednak, order booki są płytkie i istnieje spory spread, a dzienny wolumen jest znikomy na większości par.

⁶⁹ <https://cointelegraph.com/news/san-francisco-based-thor-token-project-shuts-down>

⁷⁰ <https://neotracker.io/>

⁷¹ <https://switcheroo.exchange/>

Niestety, również sam kod którym opisany jest standard NEP5 nie jest wolny od błędów i problemów. Są one naprawiane stosunkowo szybko, jednak stanowią poważny problem. Ostrzeżenie odnośnie błędów pojawiło się z ramienia Tencent⁷²⁷³, największej azjatyckiej firmy technologicznej.

Komunikat Monitoring Lab Tencent – „ Słynny projekt blockchain NEO posiada błędy wiążące się z ryzykiem zdalnego piractwa. Gdy użytkownik uruchamia węzeł sieci NEO z domyślną konfiguracją i otwiera portfel, cyfrowa waluta może zostać zdalnie skradziona.

Problem związany był z węzłami i błędami w kodzie NEP5. Kilka miesięcy później pojawił się kolejny krytyczny problem, tym razem wykryty przez organizację zajmującą się bezpieczeństwem sieciowym Qihoo 360. Błąd w kodzie pozwalał na zablokowanie całego systemu smart contractów⁷⁴

Różnego rodzaju błędy fundamentalne zostały również wykryte bezpośrednio w projektach na platformie NEO. Dotyczy to TheKey⁷⁵, DeepBrainChain⁷⁶⁷⁷ i Ontology⁷⁸⁷⁹⁸⁰. W przypadku Ontology, dodatkowo zastanawiające jest, dlaczego Li Jun – początkowo jeden z głównych deweloperów NEO, założył własną firmę – właśnie Ontology i porzucił tym samym pracę dla NEO. Daleki jestem od szukania jakichkolwiek konspiracji, jednak jest to zastanawiające.



Rysunek 27: Oryginalny post na Bitcointalk z ICO Antshares

⁷² <https://www.cryptoglobe.com/latest/2018/12/neo-vulnerability-allows-hackers-to-steal-users-tokens-chinas-tencent-warns/>

⁷³ <https://bitcoinexchangeguide.com/neo-aka-chinese-ethereum-falls-victim-to-hackers-in-new-scam-to-steal-users-coins/>

⁷⁴ http://blogs.360.cn/post/neo-runtime_serialize-dos.html

⁷⁵ <https://blog.zerononcense.com/2018/10/06/archiving-what-a-disaster-thekeys-ico-was/>

⁷⁶ <https://blog.zerononcense.com/2018/10/06/debunking-deepbrain-chain/>

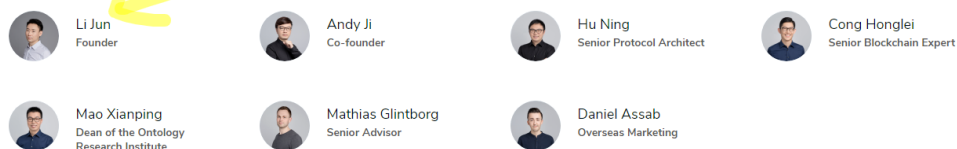
⁷⁷ <https://blog.zerononcense.com/2018/12/16/why-the-idea-of-dbc-is-utterly-implausible/>

⁷⁸ <https://blog.zerononcense.com/2018/06/22/ontology-full-research-report-6-22-2018/>

⁷⁹ <https://blog.zerononcense.com/2019/03/18/ontology-is-riddled-with-issues-pt-1/>

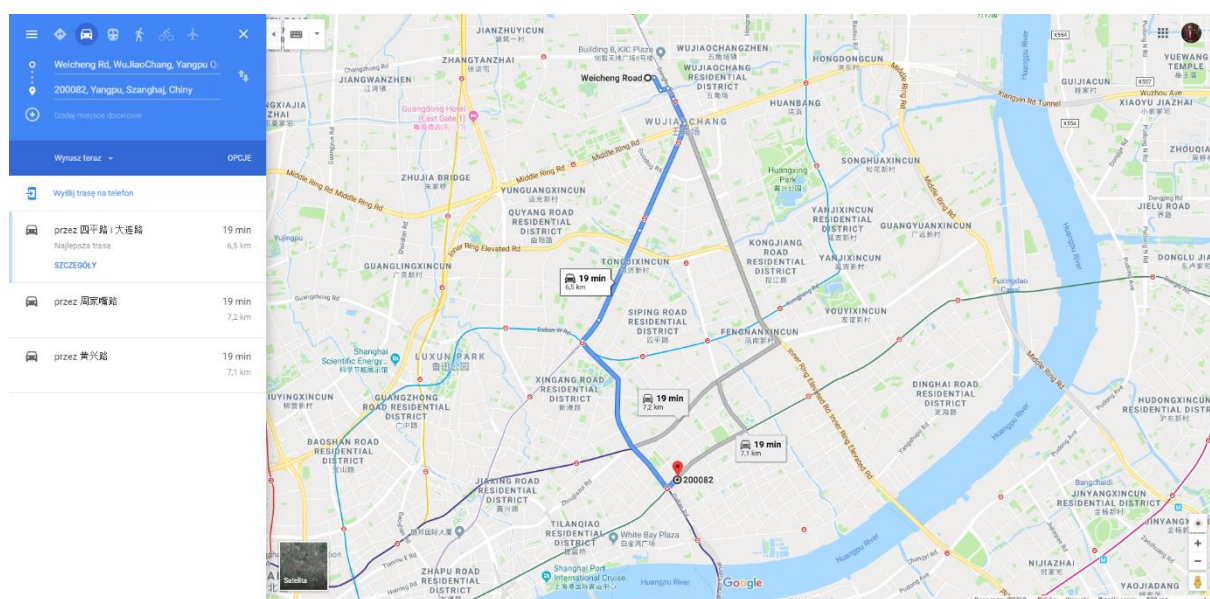
⁸⁰ <https://blog.zerononcense.com/2019/03/20/ontology-is-riddled-with-issues-pt-2/>

The Team



Rysunek 28: Grafika ze strony projektu Ontology

Być może nic nieznaczącą ciekawostką jest, że siedziby NEO i ONT dzieli jedynie 6km. Obie znajdują się w tym samym mieście, nie ma więc mowy o nieporozumieniu, zważywszy również na fakt, że ONT zdaje się nadal ściśle współpracować z NEO. Dlatego zastanawiające jest założenie przez głównego dewelopera kolejnej, tak promowanej firmy jaką jest Ontology.



Rysunek 29: Trasa jaka dzieli siedziby NEO i ONT

Ważnym wydarzeniem jest również migracja pierwszego z ICO przeprowadzonych na NEO – RedPulse – na łańcuch Binance Chain⁸¹. Co prawda projekt zarzeka się, że rozwój na NEO dalej będzie prowadzony, a obowiązywać będą dwa tokeny, w obu sieciach. Wicie już jednak co sędzę o modelu dwutokenowym. Dodatkowo w takiej sytuacji, korzyść ekonomiczna z przejścia na Binance Chain jest zaskakująco widoczna i jasna.

NEO, Onchain, DNA

O Onchain pisałem już w pierwszych akapitach. Firma założona przez współzałożyciela NEO – Da Hongfei, miała na celu stanie się prywatną firmą rozwijającą komercyjne blockchaine, w przeciwieństwie do Fundacji NEO które jest organizacją non-profit i NEO które jest oficjalnie

⁸¹ <https://blog.red-pulse.com/red-pulse-integrates-with-binance-chain-de9b5cf37030>

przedstawiane jako projekt społecznościowy. Na ten cel właśnie zebrano \$4.5M USD między II i III ICO NEO. Spójrzmy jednak jak Da Hongfei opisuje cel Onchain:

“Our vision is to make Onchain a truly universal Blockchain framework,” said Da Hongfei, founder and CEO of Onchain and creator of Antshares. “Utilizing different plug-in modules, our framework could be applied for a public chain, a consortium chain or even a private chain. Our cross-chain adaptor module, currently under development, creates interoperability among these different chains.” Da HongFei, Oct 5th, 2016.

Rysunek 30: Wizja Onchain

Czy nie są to dokładnie te same założenia co w przypadku NEO? Uniwersalny blockchain? TOP 1 do 2020 roku? W wątpliwość może być również podawany sens prywatnej zbiórki kapitału. Z artykułu projektu DNA⁸², który stanowił podstawę architektury Onchain, dowiadujemy się, że:

„Produkt, zwany DNA [Distributed Networks Architecture], jest bardzo podobny do NEO, ale został napisany w języku Go. Onchain pomaga innym blockchainom i instytucjom finansowym w tworzeniu ich blockchainów z DNA. Zasadniczo jest bardzo podobny do NEO, a w przyszłości dzięki NEOx (cross chain protocol) wszystko można będzie połączyć.”

W świetle takich informacji:

Onchain, a start-up that utilizes an open-source distributed network architecture (DNA), previously developed the public blockchain network NEO. Formerly known as Antshares, NEO raised more than more than \$4.5 million in an initial coin offering (ICO) last fall.

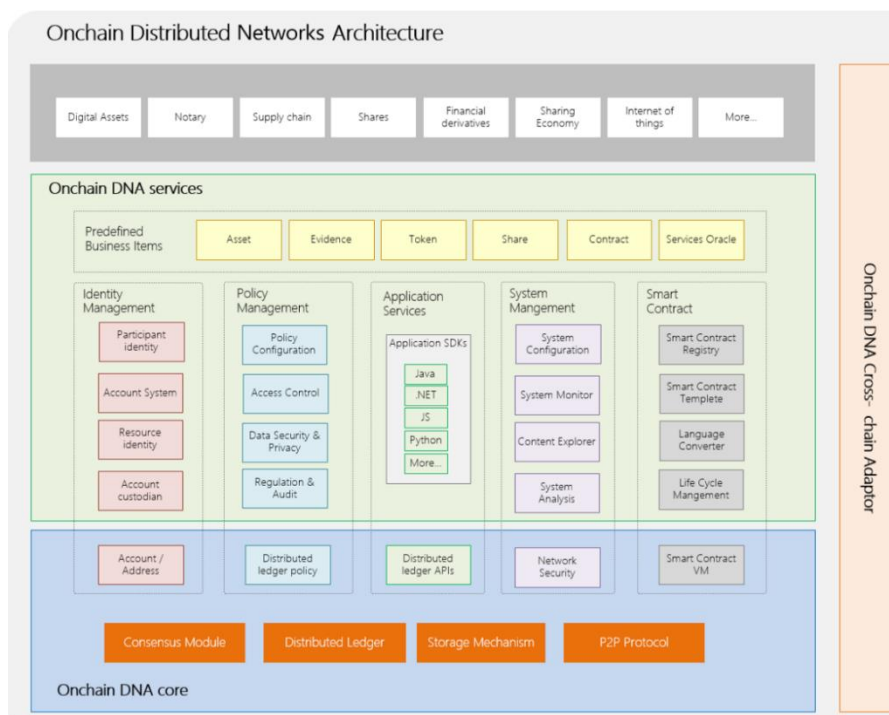
Rysunek 31: Onchain do 2017 roku zajmował się rozwojem NEO

Dziwi fakt, że Onchain, mający rozwijać prywatne blockchaine przy pomocy architektury DNA (patrz poniżej), prywatny projekt finansowany w dużej mierze przez chińską grupę Fosun⁸³, w rzeczywistości rozwijał NEO. Można wyciągnąć z tego wnioski, że Onchain, w rzeczywistości stał się po prostu prywatnym ramieniem Fundacji NEO, dzięki któremu mogli pozyskać środki na rozwój NEO, poza trzema publicznymi ICO które przeprowadzili.

Onchain jest zatem nie tylko konkurencją dla NEO. Onchain był częścią NEO. W najgłębszym tego słowa znaczeniu. Prywatnym ramieniem projektu NEO.

⁸² https://medium.com/@onchain_dna/understanding-the-onchain-neo-relationship-why-you-should-care-b8e69649ef98

⁸³ <https://neonewstoday.com/interviews/translation-of-da-hongfei-interview-on-fosun-investment/>



Rysunek 32: DNA - fundament technologii Onchain

Analizując trochę dalej ten ślad, natrafiłem na dziwną rzecz. Wszystkie oficjalne strony, strona główna jak i forum projektu DNA są nieaktywne⁸⁴. Porzucone jest również repozytorium na Githubie⁸⁵.

Sytuacja uległa zmianie, kiedy to w 2017 roku Onchain powołało projekt Ontology⁸⁷. Zagmatwana sprawa? Owszem. Zdaje się więc, że od 2017 roku, Onchain porzucił pracę nad NEO i zajął się budową Ontology – które przecież zaczynało jako token NEP5, właśnie na platformie NEO. Należy jednak przyznać, że Ontology nie przeprowadziło ICO. Tokeny zostały rozdysponowane posiadaczom NEO. Nic dziwnego, przecież Onchain już raz sfinansował swój rozwój.

Ciekawostka: NEO można wysyłać i odbierać za darmo, giełda Binance nie bierze również żadnych opłat za deponowanie i wyciąganie NEO ze swojej giełdy. Poniższy wykres pokazuje, że NEO używane jest w przeważnej mierze do przesyłania darmowych transakcji między giełdami, bez płacenia za to. Schemat jest następujący. Wpierw zakupiony zostaje Tether, później wymieniany jest na NEO, które następnie służy do darmowej transakcji i zakupu BTC na kolejnej z docelowych giełd.

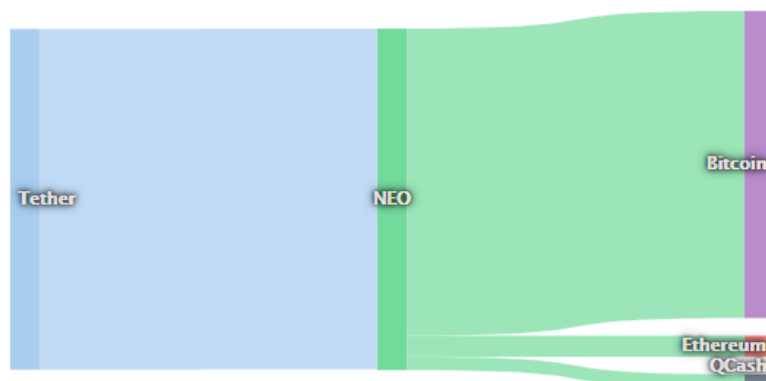
⁸⁴ <https://www.dnaproject.org/>

⁸⁵ <http://forum.dnaproject.org/>

⁸⁶ <https://github.com/DNAProject/DNA>

⁸⁷ <https://cryptobriefing.com/what-is-ontology-introduction-to-ont-token/>

Money flow from/to NEO in the last 24 hours



Rysunek 33: Money flow 24h NEO

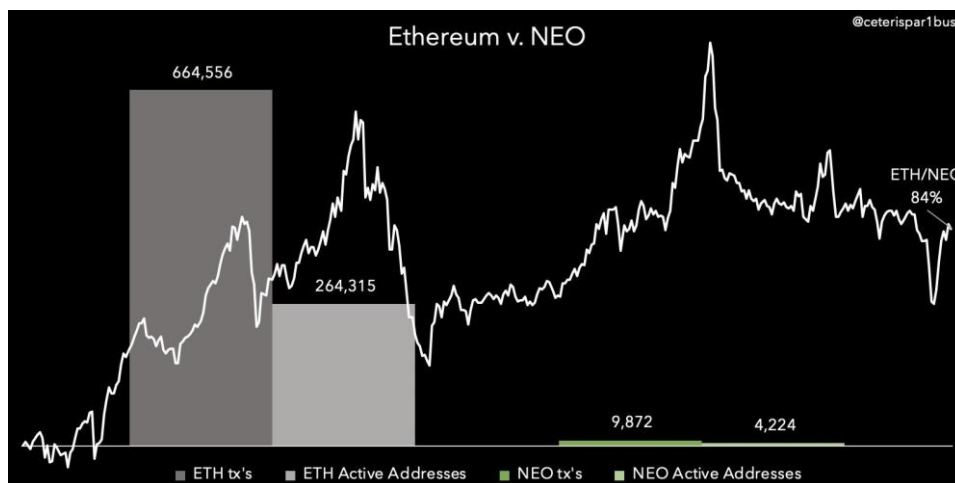
NEO w porównaniu z Ethereum

Przeciwnie do planów Da Hongfei, istnieje duże prawdopodobieństwo, poparte danymi, że NEO niestety nie zbliży się nawet do skali sieci Ethereum w najbliższym czasie.



Rysunek 34: Analiza wykonana przez Ceteris Paribus

Jak można zauważyć, aktywność w sieci Ethereum jest znacząco wyższa, niż ma to miejsce w przypadku organicznej aktywności sieciowej u NEO. Znacząco zmienił się również poziom aktywnych adresów. Spadek giełdowej wyceny wartości NEO odbił się również na ilości aktywnych użytkowników.



Rysunek 35: Analiza NEO w stosunku do ETH

Podsumowanie raportu

Raport ten miał na celu wnikliwą analizę kryptowaluty NEO, jej słabych i mocnych stron, całego ekosystemu, technologii i możliwych komplikacji długofalowych. Jest to pierwsza tak obszerna i wnikliwa publikacja dostępna publicznie w internecie na temat NEO. Część z kluczowych wniosków zaprezentowanych w raporcie jest nowa i po raz pierwszy „wychodzi” na światło dzienne. Niektóre z konwersacji między deweloperami na temat NEO 3.0 przedstawionych w tym raporcie i implikacji z nich wynikających, są unikatowe.

Raport stanowi również obszerne kompendium wiedzy na temat NEO oraz kryptowalut i mechanizmów ich funkcjonowania w ogóle. Pomimo swojej długości, każda linijka została w nim przemyślana, a żadne słowo nie zostało napisane na marne. Jeżeli jesteś zainteresowany podobnym opracowaniem na temat innej z kryptowalut, lub potrzebujesz analizy zagadnienia, bądź tematu związanego z kryptowalutami, na samym początku znajdują się dane kontaktowe. Opracowanie takiego dokumentu zajmuje ogrom czasu, więc jeżeli okazał się on dla ciebie w jakiś sposób pomocny, rozważ dotację. Wszystkie ze środków uzyskanych w ten sposób przeznaczone zostaną na dalszą pracę w tym obszarze.

Moim długoterminowym celem jest edukacja Polaków z zakresu kryptowalut. Wiąże się to z, między innymi, dostarczaniem rzetelnych i sprawdzonych informacji. Dlatego, jak mogłeś zauważyć, każde ze stwierdzeń czy argumentów podparte jest obszerną, dostępną publicznie, bibliografią. Żadne z twierdzeń przedstawione w tym raporcie, nie zostało zmyślane, bądź sfalszowane, zatajone. Wszystkie fakty możliwe są do weryfikacji osobistej, czy to za pomocą źródeł dostarczonych przeze mnie, czy własnych znalezisk.

Jeżeli udało Ci się dotrzeć do końca – Gratulację. Niezmiernie mnie to cieszy!

Pamiętajcie, kryptowaluty to niesamowity fenomen, jednak do ich pełnego zrozumienia nie wystarczy spoglądać czasem na kursy giełdowe. Potrzebne jest, przede wszystkim, zrozumienie. Technologii jak i rynku. Oby każdy z raportów prezentowanych przeze mnie przybliżał was do tego celu. Proszę również, uszanuj moją pracę i nie zmieniaj niczego w tym raporcie. Możesz go za to całkowicie dowolnie rozprowadzać między znajomych zainteresowanych kryptowalutami, lub chociażby wydrukować i umieścić w honorowej ramce na ścianie!

stokarz

