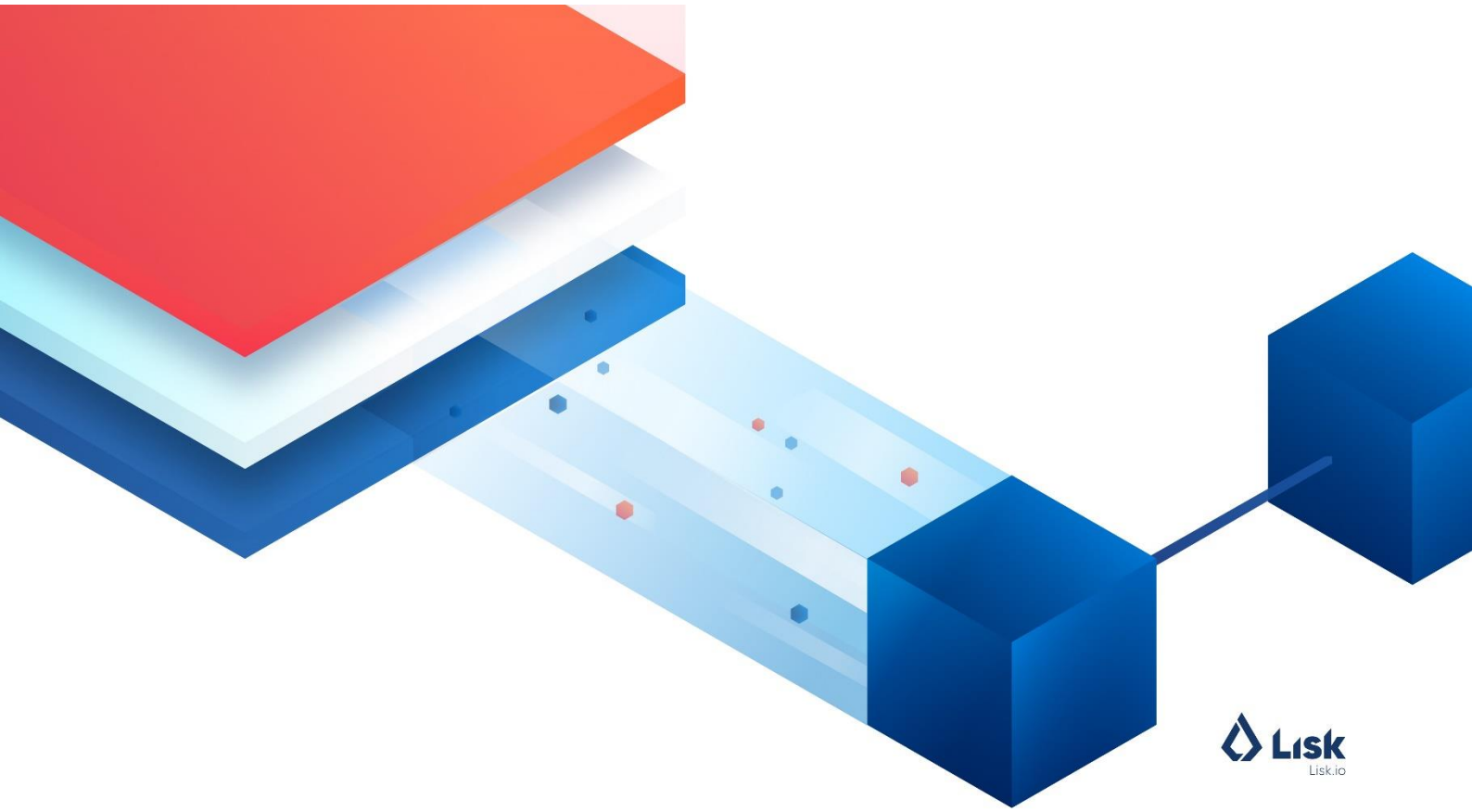
15 MAJA
2019

LISK (LSK) - RAPORT

Odkrywając potencjał technologii **Sidechain**

W zdecentralizowanych aplikacjach



Autor: stokarz

Wprowadzenie

Podejmując się analizy kryptowaluty LISK (LSK) wiedziałem, że czeka mnie niełatwe zadanie. W Polsce, jak nigdzie indziej na świecie, LISK cieszy się gigantycznym wręcz zainteresowaniem. Stało się to głównie za sprawą dostępności owej kryptowaluty na, niegdyś Polskiej, giełdzie Bitbay. Dla inwestorów LISK stanowił tańszą alternatywę dla kryptowalut takich jak Bitcoin, czy Ethereum.

Właśnie z uwagi na ogromną popularność LSK oraz liczbę osób będących pośrednio (za sprawą udzielania się w społeczności LISK) lub bezpośrednio (jeśli posiadają kryptowalutę lub należą do delegatów) zaangażowanych w projekt, dołożyłem wszelkich starań w celu przeprowadzenia skrupulatnej, rzetelnej i możliwie obiektywnej analizy. Choć każde z twierdzeń poparte jest możliwie bogatą bibliografią, zastrzegam sobie prawo do popełnienia błędów, z uwagi na fakt jak skomplikowane kryptowaluty rzeczywiście są. Pomimo sporego doświadczenia, każdy projekt jest inny i nie ulega wątpliwości, że nie wszystkie dane o każdym aspekcie projektu są publicznie dostępne.

Zanim przystąpię do jakiejkolwiek analizy własnej, przeglądam wpierw dokładnie wszystkie możliwe artykuły i opracowania o danej kryptowalucie, zarówno w języku polskim jak i angielskim. Mogę zatem szczerze powiedzieć, że w Wasze ręce przekazuje dotychczas największy raport i kompendium wiedzy o kryptowalucie LISK (LSK), jaki dostępny jest publicznie. Analizie poddane zostały niemal wszystkie aspekty projektu, wiele z wniosków, do jakich doszedłem w czasie raportu, jest unikatowa i mam nadzieję pomoże Wam w uformowaniu własnego zdania o LISK.

Zachęcam również do podejmowania dyskusji, kiedy już raport zostanie upubliczniony. Pamiętajcie, że celem moich analiz nie jest zdyskredytowanie jakiejkolwiek kryptowaluty, lecz spojrzenie na nią z lekka krytycznym i sceptycznym wzrokiem, zadanie pytań, które jeszcze nigdy zadane nie zostały, sprawdzenie ich słuszności i wyciągnięcie wniosków.

Nowość:

Piękne oprogramowanie i design nie zmienią jednak rzeczy najważniejszej – twój projekt musi mieć sens z punktu widzenia biznesowego. Nawet budując otwarty i zdecentralizowany system, sprzedajesz ludziom lub przyszłym użytkownikom pewien produkt. Jeżeli nie jest on przemyślany, to bez względu na to, jak fascynujący jest twój kod i ile pracy włożonej zostało w przygotowanie każdego aspektu projektu, jego rozwój mija się z celem. Nawet rozproszone kryptowaluty są same w sobie pewnym produktem lub w oparciu o takowe się go buduje. W przypadku Bitcoina produktem, który przyciągnął miliony użytkowników i entuzjastów z całego świata, jest pieniądz. Pieniądz wolny, bezpieczny i uniwersalny dla każdej osoby na świecie.

Nową rzeczą zastosowaną w tym raporcie jest zatem surowa analiza projektu pod kątem biznesowym. Oczywiście w przypadku niezwykle młodej i nowoczesnej technologii

kryptowalut ciężko jest stawiać jasne tezy biznesowe, gdyż zazwyczaj są to produktu, które nigdy wcześniej nie istniały. Z uwagi na to nie wiadomo, jaka jest potencjalna baza klientów zainteresowanych określonym rozwiązaniem oferowanym przez kryptowaluty. Niemniej, w przypadku projektu takiego jak LISK, który posiada trzy letni staż na rynku oraz jasną, zdefiniowaną wizję co do produktu (sidechainy), jesteśmy w stanie spojrzeć na podobne technologie tego typu, lecz oferowane przez inne projekty. Następnie sprawdzić aktualne zainteresowanie nimi – dobrą poszlaką będą dla nas chociażby ilość transakcji, czy ulokowany kapitał w łańcuchach pobocznych.

Poniżej znajdują się kluczowe wnioski wynikające z raportu, jednak wiele z omawianych zagadnień technologicznych jest niełatwa – w celu poprawnego ich zrozumienia i zinterpretowania wniosków zalecam przeczytanie pełnego raportu. Obiecuję Wam, czyta się go szybciej, aniżeli pisze! **Uszanuj moją pracę – raport można swobodnie rozpowszechniać i dystrybuować: jest on publiczny, zabrania się jednak wprowadzania zmian bądź przypisywania sobie mojej pracy.** Jeżeli jego treść pragniesz umieścić na swojej stronie, skontaktuj się ze mną. Możesz również swobodnie linkować go jako źródło.

Serdecznie zapraszam stokarz

O autorze

Zajmuję się analizą i badaniem rynku oraz technologii kryptowalut. Raporty mojego autorstwa mają charakter prywatnej opinii, nie stanowią porad inwestycyjnych. W celach współpracy proszę o kontakt:

E-mail: stokarzlol@gmail.com

Telegram: @stokarz

Kluczowe wnioski:

- LSK nie jest kryptowalutą, a tokenem użytkowym.
- Rzeczywista aktywność sieci jest niezwykle niska – transakcja wpada średnio co 7 bloków.
- **LISK będąc platformą do sidechainów nie posiada ani jednego sidechainu.**
- Sidechainy nie zapewniają nieskończonej skalowalności, są również drogie w zbudowaniu i zabezpieczeniu.
- Flagowy produkt i technologia LISK – SDK oraz sidechainy, pomimo trzech lat rozwoju, nie zostały jeszcze zaprezentowane nawet w wersji Alpha.
- Jedyna funkcjonalność tokenu LSK to wysyłanie i odbieranie, głosowanie na delegatów i handel na giełdach.
- Aktualni delegaci LISK są w stanie utrzymać swoją władzę w sieci, dzięki kontroli znaczącej ilości podaży tokenów LSK.
- W ciągu ostatnich 3 miesięcy, zaledwie 5% wszystkich adresów LISK pozostawała aktywna.
- Portal Lisk Academy jest zrobiony rewelacyjnie i stanowi świetne źródło edukacyjne.
- LISK posiada jeden z najlepszych designów wśród kryptowalut.

Ogólna ocena projektu:

5.5/10

Ostrzeżenie - ocena projektu stanowi subiektywną opinię autora i nie może wpływać na czyjąkolwiek decyzję inwestycyjną. Metryka wykorzystana w sformułowaniu oceny końcowej jest prywatna, jednak podczas ewaluacji sprawdzane są takie czynniki jak, np.: produkt, tokenekonomia, zespół, realne zastosowanie, rzeczywista aktywność sieci, partnerzy, klienci, design i wiele innych. W przypadku LISK kluczową rolę w przyznaniu tak niskiej oceny miał fakt, że pomimo upływu trzech lat, nie została wypuszczona nawet wersja Alpha kluczowego produktu, co sprawia, że LISK nie posiada żadnej funkcjonalności.

Najważniejsza część raportu znajduje się w sekcji o sidechainach i analizie aktywności sieci. Jeżeli więc jesteś dobrze obeznany z projektem LISK, polecam Ci przede wszystkim przeczytać tę część raportu. To właśnie z niej pochodzi większość kluczowych wniosków.

LISK – ZDECENTRALIZOWANE APLIKACJE

LISK to zasilany przez Java Script projekt wykorzystujący technologię sidechainów w celu rozwiązania problemów skalowalności blockchainu i zbudowania przyjaznej dla deweloperów platformy do zdecentralizowanych aplikacji – w skrócie dApps.

LISK do osiągnięcia globalnego konsensusu sieciowego wykorzystuje protokół dPOS – Delegated Proof of Stake – rodzaj POS z delegatami, którzy wybierani są poprzez demokratyczne głosowanie, zabezpieczają sieć LISK i tworzą kworum potwierdzające wszystkie transakcje. W blockchainie LISK aktywnych jest 101 delegatów. W każdej chwili nowy delegat może zostać wybrany. Każdy użytkownik jest w stanie oddać głos na delegatów – moc głosu proporcjonalna jest do ilości posiadanych tokenów – koszt głosu to 1LSK.

Dokładna ilość TPS blockchainu LISK nie jest określona, jednak różne źródła podają, że LISK jest w stanie procesować 25 TPS[1], co jest ilością zdecydowanie wystarczającą, dzięki której nie musimy poświęcać decentralizacji sieci na rzecz przepustowości. Blok propagowany jest co 10 sekund. 101 bloków (17min.) stanowi jedną „rundę", w czasie której delegaci mogą dodać jeden dodatkowy blok do sieci, za co otrzymują nagrodę.

Inicjatywą ekonomiczną dla delegatów posiadających węzły są tokeny LSK, które otrzymują w procesie nazywanym „forging". Jest on odpowiednikiem kopania waluty w blockchainie wykorzystującym protokół DPOS. Forging kontrolowany jest przez delegatów. LSK jest zatem inflacyjny. Inflacja zmniejsza się z roku na rok, aż do osiągnięcia nagrody 1LSK za blok i ustabilizowania na poziomie 2.19% w skali roku.

Większość nagród dla delegatów rozdysponowywana jest między głosujących na nich użytkowników, dzięki czemu oni również mogą otrzymywać pasywny dochód z trzymania w swoich portfelach LSK.

[1] https://www.reddit.com/r/Lisk/comments/94yf71/lisk_tps_and_scaling/

Historia Lisk

LISK założony został w 2016 roku na bazie kodu źródłowego nieistniejącego już projektu Crypti (XCR). Założycielami LISK są wieloletni entuzjaści technologii kryptowalut - Max Kordek i Oliver Beddows. Ich wizją było stworzenie platformy zapewniającej deweloperom z całego świata możliwość prostego uruchomienia własnego blockchainu, jako drugiej warstwy do głównego łańcucha LISK, tym samym tworząc niską „barierę wejścia" w kryptowaluty. Z założenia, LISK miał osiągnąć ten cel przy pomocy trzech filarów:

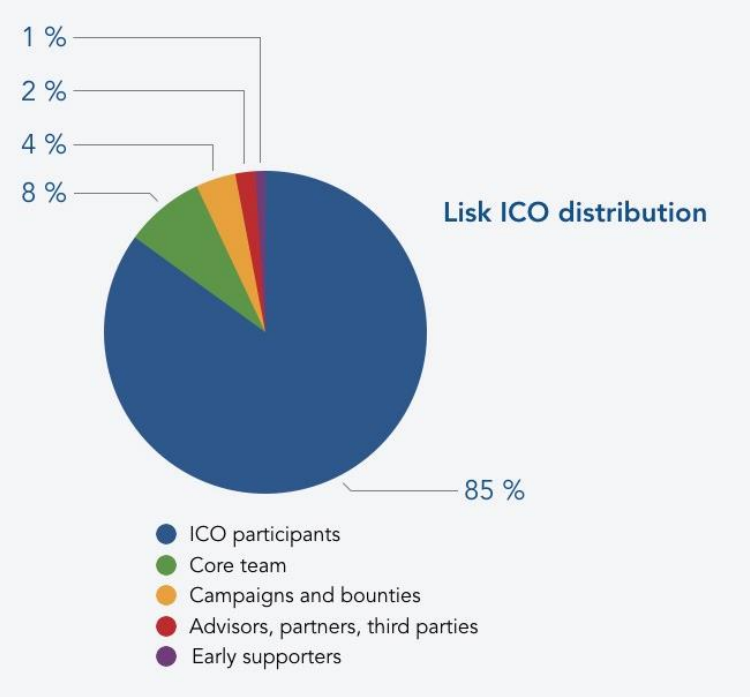
- Dostępności – korzystając z takich narzędzi deweloperskich jak SDK – Sidechain Development Kit
- Skalowalności– dzięki wykorzystaniu technologii łańcuchów dziecięcych (inna nazwa na sidechain)
- Prostego designu i rozpowszechnienia edukacji – Lisk Hub oraz inicjatywy takie jak Lisk Academy

W roku 2016 odbyło się również oficjalne ICO[2] projektu LISK. Trwało one od 22 lutego i zakończyło 21 marca. W czasie ICO doszło do ataku DDOS, który nie zagroził jednak długofalowej stabilności projektu. Jeżeli chciałeś zakupić tokeny LSK, mogłeś do tego celu użyć Bitcoina, wszystkich innych kryptowalut obsługiwanych w tamtym czasie przez Shapeshift i kryptowaluty Crypti. Poniższy wykres przedstawia schemat alokacji tokenów LSK w czasie ICO. Dużym plusem jest fakt, że aż 85% tokenów rozdysponowanych zostało pomiędzy uczestników ICO, zapewniając tym samym dobre podwaliny pod przyszły proces decentralizacji.

Ciekawostka: Max Kordek był również doradcą strategicznym w projekcie SONM[3]

Lisk doczekał się także swojego własnego forka w postaci kryptowaluty Rise[4].

[2] https://blog.lisk.io/lisk-ico-terms-25ca3ecd5a4d
[3] https://medium.com/@MaxKordek/advising-sonm-586da71e93e2
[4] https://steemit.com/rise/@lexiconical/rise-a-formerly-promising-lisk-fork-that-crashed-93-in-february-crypto-collapse



Rysunek 1: Alokacja tokenów LSK

Również na plus jest transparentność założycieli projektu – Maxa Kordka i Oliviera Beffowa – którzy 18 miesięcy po ICO opublikowali[5] publiczne oświadczenie przedstawiające dokładnie, jak wyglądać będzie strategia sprzedaży tokenów LSK przez nich posiadanych. Tabela przedstawia ilość tokenów które mogą sprzedać założyciele LISK wraz z upływem czasu.

Time	Liquidation	LSK left	Years in
2016 Q4	0	2.000.000	1
2017 Q2	300.000	1.700.000	1,5
2017 Q4	170.000	1.530.000	2
2018 Q2	153.000	1.377.000	2,5
2018 Q4	137.700	1.239.300	3
2019 Q2	123.930	1.115.370	3,5
2019 Q4	111.537	1.003.833	4
2020 Q2	100.383	903.450	4,5
2020 Q4	90.345	813.105	5
2021 Q2	81.310	731.794	5,5
2021 Q4	73.179	658.615	6
2022 Q2	65.861	592.753	6,5
2022 Q4	59.275	533.478	7
2023 Q2	53.348	480.130	7,5
2023 Q4	48.013	432.117	8
2024 Q2	43.212	388.905	8,5
2024 Q4	38.891	350.015	9
2025 Q2	35.001	315.013	9,5
2025 Q4	31.501	283.512	10

Rysunek 2: Upłynnienie tokenów założycielskich LSK

[5] https://medium.com/@MaxKordek/liquidation-strategy-60f055d75049

Finansowanie projektu

Finalnie LISK był w stanie zebrać 14 009 BTC i 80 mln XCR, co odpowiadało ponad $6 mln USD. Na tamte czasy, było to drugie największe ICO w historii, zaraz po udanym debiucie Ethereum.

Funduszami od czasu ICO zarządza, znajdująca się w Szwajcarii, Fundacja Lisk. Jest ona organizacją non-profit. Ramieniem rozwojowym LISK jest, oprócz małej grupy niezależnych deweloperów społecznościowych, prywatna berlińska spółka Liqhtcurve, studio deweloperskie blockchain powołane i zarządzane przez założycieli LISK. Wszelkie zmiany w publicznej sieci LISK dokonywane są za pomocą LIP – LISK Improvement Proposal – odpowiednikowi systemu BIP znanego z Bitcoina. Propozycja zmian przedstawiana jest przez deweloperów na platformie Lisk Research, gdzie następnie przeprowadzane jest demokratyczne głosowanie.

Fakt, że jedynym produktem LISK, w dodatku niedostępnym jeszcze na rynku, są sidechainy i narzędzia SDK, może nieco martwić. W żadnym momencie w czasie, projekt LISK nie ma zamiaru „zarabiać na siebie". Wiedząc, jak wysokie są koszty opłacenia licznego grona pracowników technicznych – obecnie nad rozwojem LISK pracuje na stałe 57 pracowników[6], może być to niepokojące. Jedynym więc sposobem opłacenia dalszego rozwoju LISK jest sprzedaż tokenów posiadanych przez Fundacje na wolnym rynku, jednocześnie licząc na sukces projektu i wzrost giełdowej wartości tokenu LSK.

Kod źródłowy LSK pisany przez studio Lightcurve jest zdecydowanie najwyższej jakości, co potwierdza niedawny raport firmy Darpal Rating[7] zajmującej się audytem kodów kryptowalut i ich ewaluacją.

[6] https://lightcurve.io/about-us?positions=

[7] https://medium.com/@DPRating/darpalrating-github-audit-for-200-blockchain-projects-march-2018-3c6b839abdaa

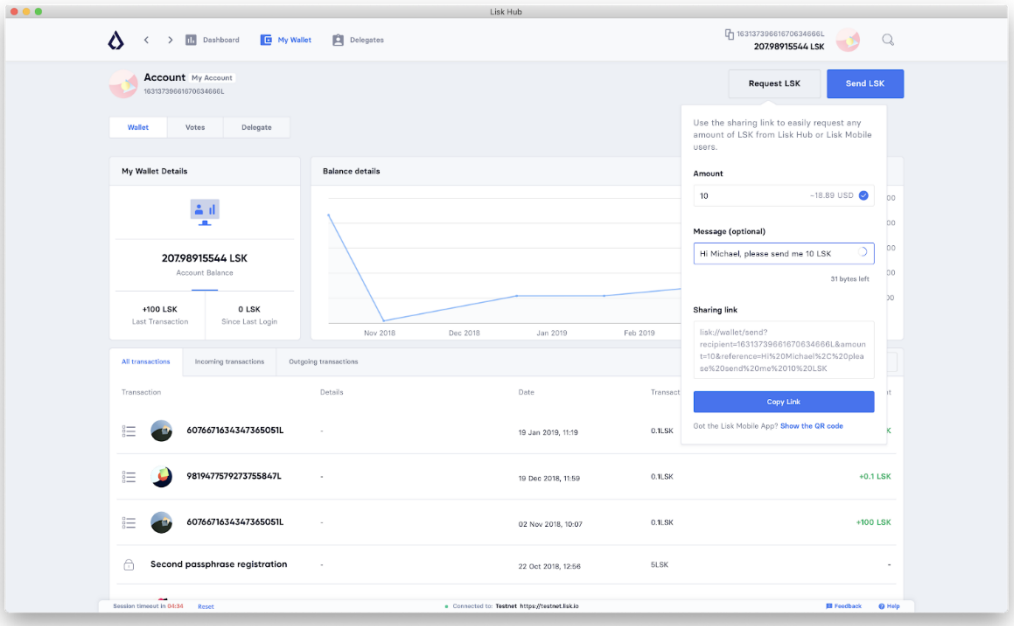
Społeczność

Społeczność LISK jest imponująca, jak na projekt, który nie wydał nawet swojego flagowego produktu. Szczególnie w Polsce zainteresowanie LSK jest ogromne, co powiązać można z dostępnością projektu na giełdzie Bitbay, oferującej bramkę wymiany kryptowalut w stosunku do PLN.

Rysunek 3: Statystyki obrazujące wielkość społeczności LISK

LISK posiada dużą bazę obserwujących na Twitterze i Reddicie – dwóch najważniejszych mediach zrzeszających społeczność kryptowalut. Odpowiednie ich wykorzystanie powinno być fundamentem marketingu LISK, gdyż, szczególnie Twitter, oferuje wspaniałą dźwignię, dzięki której o LISK mogą dowiedzieć się setki tysięcy potencjalnych użytkowników i deweloperów przeglądających Twittera każdego dnia.

Ekosystem LISK



Rysunek 4: LISK HUB

Ekosystem LISK jest niewielki i składa się z:

- LISK HUB – aplikacji ALL-IN-ONE dla użytkowników i deweloperów – należy pochwalić ją za fenomenalny interfejs graficzny i intuicyjność, dwie rzeczy których kryptowalutom zdecydowanie brakuje
- LISK Academy – fenomenalnej inicjatywy o pierwszorzędnym wykonaniu. Jako osoba, która sama wspiera edukacje z zakresu kryptowalut w Polsce, mogę z czystym sercem powiedzieć, że Akademia Liska stanowi jedno (zaraz obok Binance Academy) z najlepszych źródeł wiedzy o kryptowalutach, zarówno dla początkujących, jak i zaawansowanych. Jest stworzona zadziwiająco obiektywnie, każdy z krótkich artykułów wyjaśnia w świetny sposób skomplikowane zagadnienia kryptograficzne. Myślę, że na tą chwilę Akademia Lisk stanowi unikatowy i najmocniejszy atut całego projektu LISK. Nie zapominajmy jednak, że jest to inicjatywa drugorzędna. LISK nie jest przecież platformą edukacyjną.
- LISK Commander
- LISK Explorer
- LISK Elements
- LISK Core
- *SDK – nie ukończonego, flagowego produktu LISK. Prace nad nim trwają nieprzerwanie od trzech lat, data wprowadzenia jest nieznana*

Wizja długofalowa

Rysunek 5: Roadmap LISK

Problemami, które LISK pragnie rozwiązać są: skalowalność, niska wiedza odnośnie kryptowalut i trudność w budowaniu systemów opartych na blockchainie.

Z wysoką pewnością można założyć, że popyt na tego typu usługi, wraz z ogólnym rozwojem rynku kryptowalut będzie wysoki. Na razie jednak marketing LISK nie odzwierciedla rzeczywistego stanu rozwoju projektu, co zostało potwierdzone przez członków zespołu[8], dlatego jeżeli chcemy mówić o jakiejkolwiek większej adopcji, kluczową rzeczą jest poczekać na finalną wersję pierwszego z produktów LISK – SDK.

Możemy jednak przyjrzeć się, jak prezentuje się obecny stan sieci LISK oraz czy technologia sidechain rzeczywiście zapewnia nieskończoną skalowalność blockchainu, a czy nie jest może zwyczajnie dobrym rozwiązaniem do określonego zestawu problemów. Zapraszam zatem do części II, w której to zbadamy technologię sidechain, tokenoekonomię, aktywność sieci oraz model delegatów w protokole DPOS.

[8] https://cryptobriefing.com/lisk-devs-learn-hard-way/

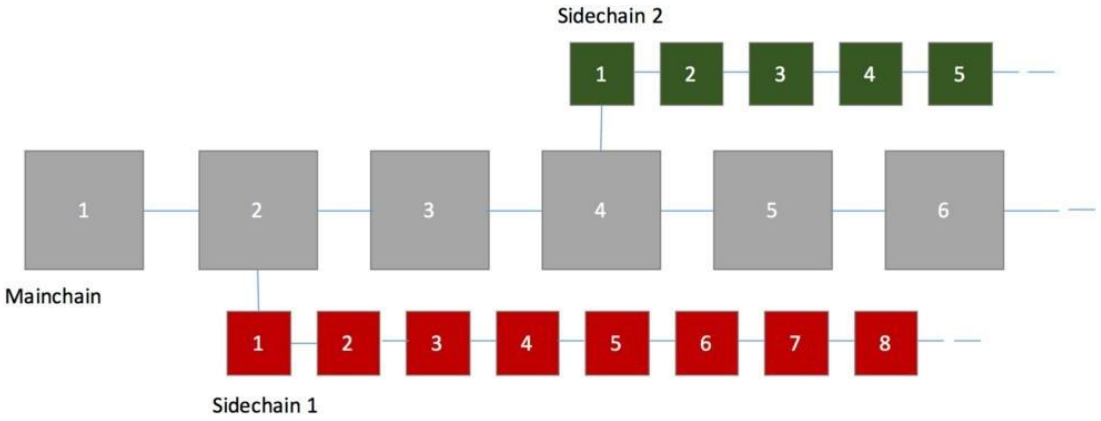
CZĘŚĆ II

Sidechains - Flagowy produkt LISK

Rysunek 6: Produkty LSK

Kluczowym atutem i zarazem największą obietnicą LISK jest technologia sidechains (albo childchains), czyli łańcuchów pobocznych. Ma być ona odpowiedzią na niską skalowalność aktualnych blockchainów. Sidechainy oraz SDK – Sidechain Development Kit – zbiór narzędzi deweloperskich, dzięki którym programiści mają, w prosty sposób, mieć możliwość budowania łańcuchów pobocznych na LISK. SDK oraz sidechains były od zawsze centralnym punktem, wokół którego skupiał się cały marketing i obietnice LISK.

To właśnie one mają zapewnić adopcję i rozpoznawalność LISKowi. Pozbądźmy się na chwilę całego szumu i przyjrzyjmy się dokładnie czym właściwie sidechainy są, skąd się wzięły i dlaczego mają być odpowiedzią na problemy z niską skalowalnością kryptowalut.



Rysunek 7: Wizualizacja łańcucha pobocznego

Sidechain[9] jest odseparowanym blockchainem działającym równolegle do łańcucha głównego. Łańcuch poboczny ma zazwyczaj charakter prywatnej sieci, z określoną formą interoperacyjności z głównym blockchainem. Największymi atutami sidechainów jest zdecydowanie fakt, że mogą mieć zupełnie inne cechy, aniżeli łańcuch główny. Zatem różnić może się protokół konsensusu – główna sieć może dochodzić do globalnej zgody za pomocą np. POW (Proof of Work – protokół znany z Bitcoina), przepustowość sieci, jej możliwości w przesyle transakcji na sekundę.

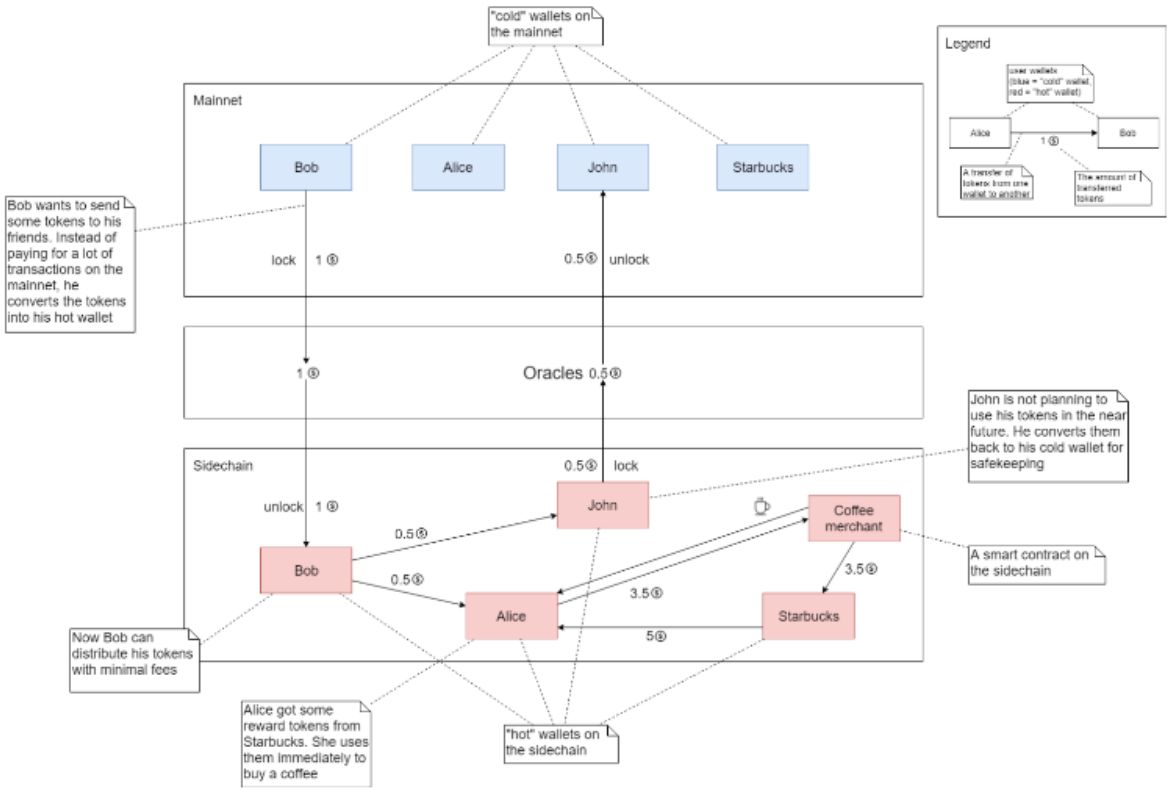
Historia łańcuchów dziecięcych

Historia sidechainów rozpoczyna się w 2014 roku, kiedy to grupa kryptografów obecnie w większości związana z firmą Blockstream[10] opublikowała dokument prezentujący koncepcję łańcuchów pobocznych: „Enabling Blockchain Innovations with Pegged Sidechains[11]". Sidechainy przedstawione zostały jako rozwiązanie niektórych problemów Bitcoina. Zamiast zmieniać całą główną sieć, można było od teraz wprowadzić sidechain – do głównego łańcucha dodać „drugą warstwę". Dzięki pewnym ustępstwom, jak zmniejszona decentralizacja w obrębie sidechainu, bylibyśmy w stanie procesować zwiększoną liczbę transakcji na sekundę lub pośrednio wprowadzić nową klasę obiektów do Bitcoina. Ważne jest, że sidechain jest całkowicie niezależny od głównego łańcucha – jeżeli jakikolwiek błąd wystąpi w jego obrębie, łańcuch główny nie zostanie narażony na niebezpieczeństwo. Ma to jednak swoje

[9] https://github.com/ambrosus/sidechannel-bridged-token-PoC/blob/master/Sidechannel+PoC+documentation.pdf
[10] https://blockonomi.com/sidechains/
[11] https://blockstream.com/sidechains.pdf

konsekwencje i jak każda technologia w kryptowalutach jest sztuką ustępstw. Sidechainy są dobrym rozwiązaniem na niektóre problemy – nie zapewnią jednak, w przeciwieństwie do tego co możemy przeczytać w licznych ogłoszeniach projektu LISK – nieskończonej skalowalności. Przynajmniej nie w takim sensie w jakim jest to reklamowane.

Sidechains – technologia ustępstw



Rysunek 8: Techniczny rysunek sidechainu

Sidechainy, dzięki niezależności od łańcucha głównego, mogą być całkowicie odmiennie zbudowane. Ich dużym plusem jest zatem plastyczność – sidechain może posiadać funkcje zapewniające prywatność użytkownika, większą przepustowość transakcji czy otwierać bramy do dotąd niedostępnej płynności przesyłania kapitału.

Błędem jest natomiast zakładanie, że wykorzystanie sidechainów w LISK pozwala na nieskończoną skalowalność. W obrębie małoskalowego projektu, jakim obecnie jest LISK, nie dostrzega się tych problemów. Zdeponowanie sidechainu wiąże się obecnie z wysokimi kosztami.

- Wpierw musimy zapewnić architekturę serwerową, która będzie stanowiła połączenie między łańcuchem głównym, a sidechainem. Nie istnieje obecnie sposób na komunikację łańcuchu głównego z sidechainem w systemie peer-to-peer.
- Sieć główna jest całkowicie niezależna od łańcucha pobocznego. Choć jest to rozwiązanie bezpieczne dla głównego blockchainu, każdy z nowo utworzonych sidechainów musi samemu zapewnić bezpieczeństwo swojej sieci. Nie może przy tym korzystać z zasobów sieci głównej, gdyż jest od niej niezależny. Dochodzi więc do sytuacji, w której mamy pewne ustępstwa. Łańcuch główny LISK jest „bezpieczny" od ewentualnych błędów na łańcuchach pobocznych, jednak same sidechainy muszą zadbać o własne bezpieczeństwo.
- Każdy z sidechainów musi powołać Federację – organ nadzorujący, zazwyczaj całkowicie scentralizowany, odpowiedzialny za propagowanie bloków i zarządzanie natywną kryptowalutą sidechainu. Na przykład, w przypadku sieci Liquid Blockstream – sidechainu Bitcoina, Federacja składa się z 15 jednostek nadzorujących.

Sidechainy powodują również kolejne problemy. Każdy sidechain potrzebuje własnej kryptowaluty. Takie rozwiązanie może być dobre w celach zbiórki kapitału dla projektu w ICO (Initial Coin Offering – odpowiednik IPO w kryptowalutach), jednak z perspektywy biznesowej jest to wielki kłopot, gdyż zdecydowanie utrudniamy nasz biznes/projekt. Aby klient/użytkownik skorzystał z aplikacji którą budujemy, musi korzystać z naszego tokenu. Dodaje to więc kolejną warstwę skomplikowania.

W świecie poza kryptowalutami, przekonanie kogokolwiek do wykorzystania Bitcoina lub Ethereum – będących najpopularniejszymi kryptowalutami, posiadającymi jednocześnie największą markę i rozpoznawalność – jest trudne. Jeśli użytkownik, w celu wykorzystania naszej usługi, musi wejść w „sferę" naszego, bardzo egzotycznego dla zewnętrznego obserwatora, tokenu, redukuje to drastycznie ilość potencjalnych klientów dla naszego biznesu.

Własny token w obrębie sidechainu ma atuty. Tak jak w przypadku LBTC w sidechainie Liquid, może służyć on do szybszego przesyłania mikrotransakcji, rezygnując z decentralizacji i bezpieczeństwa na rzecz jednego organu centralnego, który procesuje transakcje. Zatem wszelkie mikrotransakcje mogą odbywać się w LBTC, a następnie, np. kiedy zbierze się ich odpowiednia ilość, ze wszystkich wejść i wyjść w obrębie sidechainu Liquid można utworzyć jedną grupę i przetransmitować jako jedna transakcja na główny łańcuch Bitcoina. Niemniej, rezygnujemy w tym wypadku z bezpieczeństwa i wysokiej pewności rozliczenia którą posiada Bitcoin, gdyż sidechain Liquid opiera się o centralną jednostkę kontroli.

Ciekawostka: W przypadku sidechainów, również w LISK, kryptowaluta wysłana z głównego łańcucha na sidechain, w momencie wysłania jest lokowana i chwilowo niemożliwa do wykorzystania. Kiedy już dojdzie do sprawdzenia bezpieczeństwa, kryptowaluta udostępniania jest na sidechainie.

Problemem jest to, że nie wiemy obecnie, jak zachowywałby się blockchain posiadający np. 100 sidechainów. Pamiętajcie, że w zdecentralizowanej i bezpiecznej sieci, węzły każdorazowo muszą dojść do porozumienia w przypadku każdej z transakcji. Ilość operacji potrzebnych do przetworzenia przez i tak już rozproszone zasoby obliczeniowe, przy tak dużej złożoności systemu, mogłoby prowadzić do opóźnień, a nawet paraliżu sieci. Problemów tych oczywiście nie widać, jeśli system posiada zaledwie kilka łańcuchów pobocznych, a dodatkowo aktywność użytkowników jest niewielka

Sidechainy wprowadzają nieco skomplikowania do systemu. Jak widzicie, mają swoje atuty, jednak wiążą się one z ustępstwami, na które się zgadzamy. Dlaczego? Tak, jak już mówiłem, niezależność sidechainów jest atutem dla łańcucha głównego – nie jest on narażony na błędy mogące wystąpić na łańcuchu pobocznym – każdy sidechain musi samemu zapewnić sobie bezpieczeństwo. Nie jest w tym celu możliwe skorzystanie ze zgromadzonej mocy obliczeniowej na łańcuchu głównym. Co więcej, każdy sidechain zmuszony jest powołać Federację, zazwyczaj grupę kilkunastu przedstawicieli (czyli o dużej centralizacji) odpowiedzialną za propagowanie bloków i zarządzanie sidechainem. Tak więc, sidechainy są zazwyczaj o wiele bardziej scentralizowane niż ojczysty łańcuch oraz mało bezpieczne, przez co podatne na potencjalne ataki. Korzystając z sidechainów użytkownik musi zadać sobie pytanie – czy chcę porzucić zdecentralizowany i bezpieczny łańcuch główny, któremu nie mogę ufać (tak jak to ma miejsce w przypadku Bitcoina) – na rzecz sidechainu zarządzanego przez małą grupę ustalonych organizacji.

Dobrą wizualizacją ustępstw, na które jesteśmy zmuszeni pójść w przypadku sidechainów jest przykład sidechainu Liquid, o którym już wspomniałem. Zarządzany jest on przez konsorcjum giełd i firm takich jak Blockstream. Jednak jak pokazują dane historyczne, chociażby ostatni hack Binance, giełdy są podatne na ataki i, co za tym idzie, kradzież kryptowalut użytkowników. Bitcoin, dzięki ilości mocy obliczeniowej, która zabezpiecza łańcuch, jest stosunkowo bezpieczny w użyciu, a przeprowadzenie skutecznego ataku przy pomocy 51% mocy obliczeniowej wiązałoby się z niebotycznymi kosztami dla atakującego. W większości przypadku czyni to więc Bitcoina bezpiecznym. Nie musimy się martwić o to, że nasze środki zostaną przechwycone przez nieuczciwych atakujących. W przypadku mniej bezpiecznego sidechainu Liquid, posiadającego własną walutę – LBTC, będącą z założenia odpowiednikiem BTC na łańcuchu głównym, powierzamy swoją kryptowalutę w ręce Fundacji. To ona zarządza naszymi LBTC (odpowiednikowi BTC w łańcuchu pobocznym). Fundacja natomiast składa się z grupy giełd i firm kryptowalutowych. Giełd możliwych do zaatakowania. Giełd, które już niejednokrotnie były skutecznie atakowane i okradzione. Korzystając z sidechainu Liquid

odrzucamy bezpieczeństwo Bitcoina na rzecz prędkości transakcji. Tylko od nas zależy, czy jesteśmy w stanie pójść na tak wysokie ustępstwo i czy jest ono dla nas opłacalne.

Oczywiście, problemy z niskim bezpieczeństwem sidechainu można przezwyciężyć, a przynajmniej utrudnić potencjalnym nieuczciwym aktorom atak na sieć poboczną. Jednym z rozwiązań jest stworzenie nowej, zdecentralizowanej architektury serwerowej, rozproszonej na cały świat. Uważny czytelnik zauważy jednak od razu z jak wysokimi kosztami wiąże się takie zadanie. **Stworzenie odpowiednio bezpiecznego sidechainu jest zatem procesem kosztownym i wymagającym czasu.**

A więc tak, możemy za pomocą sidechainów skalować główny łańcuch – aby robić to w nieskończoność jak twierdzą przedstawiciele projektu LISK, musielibyśmy posiadać tylko nieskończone zasoby pieniężne, nieskończoną architekturę serwerową i nieskończenie wiele czasu, aby to wszystko zbudować. Włóżmy więc argument o nieskończonej skalowalności między bajki. Sidechainy są ciekawą technologią i warto mieć ją na uwadze. Jednak, tak jak wszystkie z rozwiązań technicznych, musi zostać zastosowana do rozwiązania odpowiedniego problemu i wiąże się z ustępstwami, na które musimy pójść.

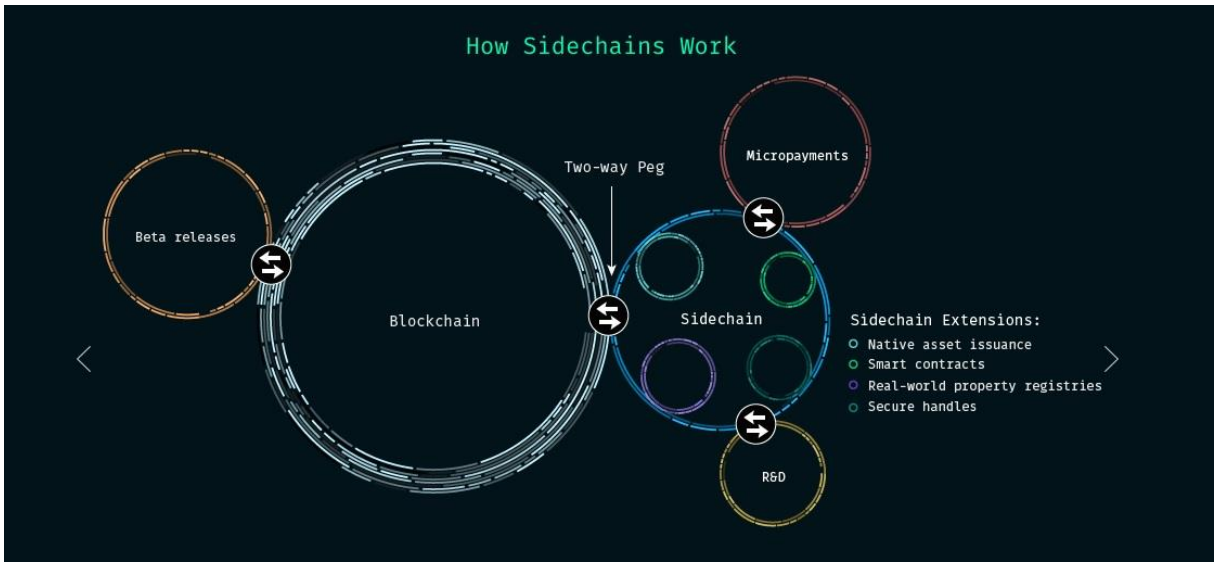
Po obszernej analizie stwierdzam, że nic nie wskazuje na to, aby sidechainy miałyby być w czymkolwiek lepsze w rozwiązaniu problemu skalowalności blockchainów od chociażby shardingu. Są zwyczajnie inną drogą, którą obieramy – kosztowną i zapewniającą innego rodzaju benefity – niekonieczną.

Przyjrzyjmy się teraz sidechains od strony biznesowej. Dlaczego? Gdyż kryptowaluty potrzebują takiego spojrzenia. Mamy rok 2019, nie 2017, minął więc czas kiedy to wystarczyło pięknie zrobione logo i kilka nowoczesnych haseł, w których zawarte były słowa blockchain najlepiej w połączeniu z Big Data i AI, aby kryptowaluta uznana została za przełomową. Czas najwyższy, aby lokować kapitał i wspierać projekty przedstawiające sobą realną szansę usprawnienia danej części naszego życia i stworzenia liczących się na świecie technologii. Prawa ekonomii aplikuje się do rynku kryptowalut tak samo, jak do każdego innego. To właśnie dzięki temu, że Bitcoin jest jednym z najlepszych pieniędzy jakie mamy, charakteryzuje się wysokim bezpieczeństwem i częściową anonimowością oraz dostępnością, nosząc zasłużone miano gotówki internetu, jest on dzisiaj wykorzystywany na całym świecie.

Sprawdzanie nowych technologii w kategoriach sensu biznesowego jest niezwykle trudne i nie zamierzam tutaj stawiać jasnych odpowiedzi. Nie można i nie powinno się mówić w „pewnościach", że dany produkt lub technologia przyjmie się na rynku bądź nie. Nie wiemy tego. Co jednak możemy zrobić, to wziąć dane odnośnie tej samej technologii, ale rozwijanej przez inne projekty, a następnie sprawdzić, jak one się przyjmują i czym różnią się od

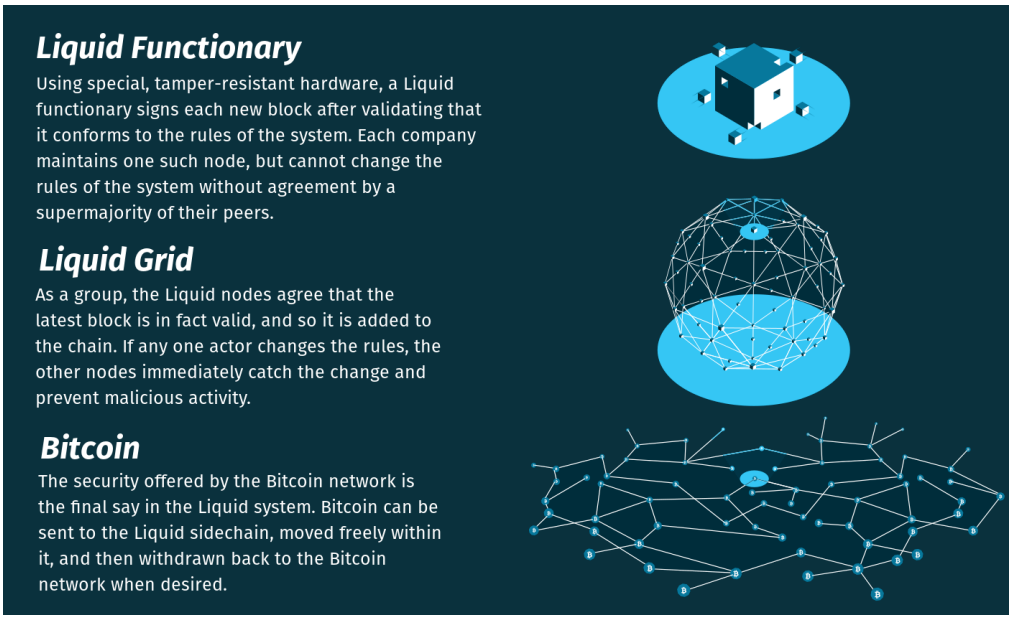
sidechainów proponowanych przez LISK. Jesteśmy również w stanie przeanalizować rynek zdecentralizowanych aplikacji (dApps) i określić, czy jest w nim miejsce dla LISK, w jego obecnej formie.

Blockstream Liquid – sidechain Bitcoina



Rysunek 9: Jak działa sidechain Bitcoina - Liquid autorstwa Blockstream

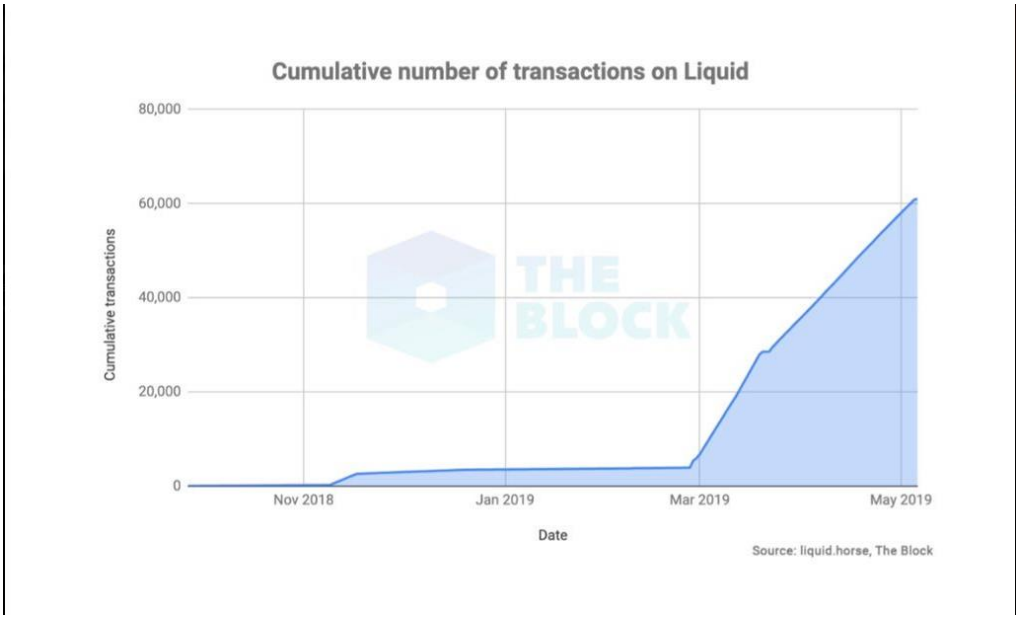
Jednym z takich przykładów jest sidechain Bitcoina – Liquid. Ma on za zadanie, dzięki integracji z największymi giełdami świata, umożliwić momentalne przesyłanie BTC w formie LBTC na sidechainie. Według założeń, klienci giełd byliby w stanie transmitować BTC z jednej giełdy na drugą w ciągu kilku sekund. Jakby to wyglądało? Dla użytkowników nic by nie uległo zmianie, jednak w systemach giełd BTC zamieniane byłyby na LBTC, następnie przesyłane poprzez sidechain na określoną giełdę. Kiedy transfer zostałby ukończony LBTC konwertowane byłyby na BTC na głównym łańcuchu.



Rysunek 10: Jak działa sieć Liquid

Blockstream jest firmą nieporównywalnie większą i bardziej rozpoznawalną od projektu LISK. Wydawałoby się więc, że popyt na sidechain Bitcoina powinien być duży. Jak jednak wygląda rzeczywistość?

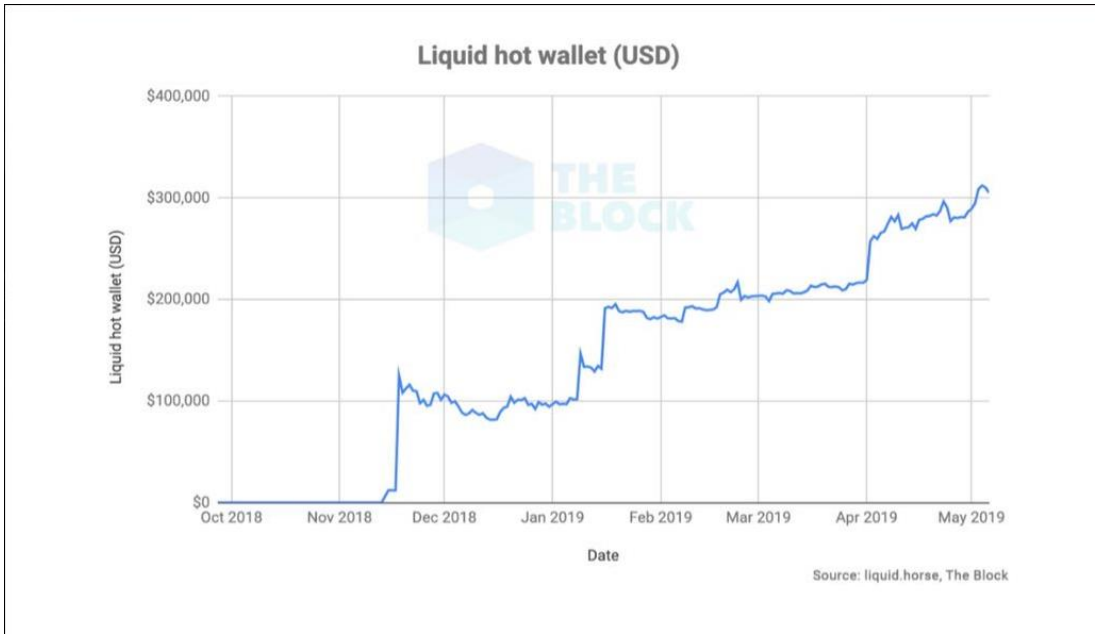
Są to dane na dzień 11.05.2019 – Liquid rozwijany jest od ponad kilku lat i tak wygląda obecna aktywność sieci. Sidechain nie został jeszcze zintegrowany ze światowymi giełdami.



Rysunek 11: Liczba transakcji na Liquid - źródło: The Block

Sieć Liquid, sidechain Bitcoina, na chwilę obecną miał jedynie 60 tysięcy transakcji. Od każdej z nich pobierana jest mikroskopijna opłata, możemy więc z wysoką pewnością stwierdzić, że koszty deweloperskie oraz zapewnienie odpowiedniej architektury serwerowej, nie zostały dotychczas zwrócone.

Transakcje w sieci Liquid, w okresie od listopada 2018 do maja 2019, odpowiadały za raptem 20% transakcji z jednego dnia na łańcuchu głównym Bitcoina. Sieć Bitcoin zatwierdza średnio 370 tysięcy transakcji dziennie[12].



Rysunek 12: Ilość $ na hot wallecie Liquid

Rysunek przedstawia ilość BTC (określoną w $) trzymaną na gorącym portfelu Liquid. Odpowiada ona ok. 40 BTC.

Dla porównania podobna technologia mająca zapewnić skalowalność Bitcoina tworząc tzw. „drugą warstwę" - Lightning Network, posiada obecnie w swojej sieci 1037 BTC[13].

Co dane te mówią nam o LISK i jego sidechainach?

Sidechainy proponowane przez LISK mają służyć zupełnie innym celom. Dane o Liquid pokazują jednak, że do rzeczywistej adopcji sidechainów nawet w obrębie społeczności kryptowalut, jeszcze daleka droga. Moim zdaniem, mówimy tutaj o minimum dwóch latach, zanim

[12] https://www.blockchain.com/charts/n-transactions?timespan=180days&showDataPoints=true&daysAverageString=7
[13] https://1ml.com/

sidechainy zaczną być rzeczywiście używane. Jeśli zaś chodzi o ich wykorzystanie w dApps może nigdy do tego nie dojść, na skalę której oczekiwałby LISK. Dlaczego? Odpowiedź już niedaleko.

Przypomnijmy, że Liquid jest prywatną siecią Blockstream – sidechainy są w większości z definicji prywatne. Sieć dąży do decentralizacji poprzez wprowadzenie do organu Federacji jak największej ilości członków. U podstaw jednak, Liquid zarządzany jest przez Blockstream. Tak więc korzystając z sidechainu Liquid, powierzamy całe nasze zaufanie jednej firmie.

Plusy i minusy sidechainów

Podsumowując, obecnymi słabymi punktami w przypadku sidechainów są: bezpieczeństwo, potrzeba ustanowienia centralnego organu zarządzania – Federacji (atak wymierzony w Federację skutecznie paraliżuje sieć) i serwerów łączących główny blockchain z łańcuchami pobocznymi, koszty oraz własny token (sidechain musi posiadać jakąś „jednostkę miary") oraz to, że Federacja kontroluje twoją kryptowalutę w obrębie ich sidechainu.

Nie wiemy również jak działa i sprawdza się architektura sidechainów w przypadku ich dużej ilości i wielu użytkowników, czynnie korzystających z sieci głównej oraz sidechainów.

Natomiast dużymi plusami są: modularność sidechainów i możliwość dostosowania ich do konkretnych problemów, jak na przykład zapewnienie większej płynności i szybkości transferów kryptowalut między dużymi, scentralizowanymi punktami jakimi są giełdy. Dodatkowo z pomocą sidechainów możemy wprowadzić różne nowinki techniczne, jako drugą warstwą do blockchainu, bez narażania głównego łańcucha na niebezpieczeństwa.

Skala rynku dApps

Sidechainy LISK nierozerwalnie wiążą się z zdecentralizowanymi aplikacjami. LISK jest platformą, na której najpierw deponujemy sidechain, aby następnie przygotować grunt pod naszą dApp. Posiadając własny token w sidechainie jesteśmy w stanie przeprowadzić ICO, zebrać fundusze i finalnie zaprezentować swoją aplikację światu.

Okazuje się jednak, że rynek dApp jest znacznie mniejszy, niż może nam się to wydawać[14]. Zdecentralizowane aplikacje stanowią jedynie marginalny wycinek całości rynku kryptowalut. Dane z końca zeszłego roku pokazują, że jedynie 20 dApps mogło pochwalić się 1000 aktywnymi użytkownikami miesięcznie[15]. DAppps cieszące się zatem największym sukcesem w skali światowej, mogą liczyć na średnio 6 transakcji dziennie.

Liczby te mogą zaskakiwać. Czy dApps nie miały być ultymatywnym celem kryptowalut takich jak Ethereum? Rzeczywistość pokazała, że użytkownicy zdecydowanie bardziej preferują klasyczne aplikacje możliwe do pobrania w App Store lub Google Play. Możemy jedynie spekulować, co jest tego powodem, gdyż nie są dostępne jasne dane na ten temat. Według mnie, ma to związek ze wczesnym stadium całego rynku kryptowalut, a także problemów jakie napotykają potencjalni odbiory dApps. Zdecentralizowane aplikacje są nie tylko obskurne w designie, lecz również posiadają wysoką „barierę wejścia". Do ich wykorzystanie potrzebujemy rozszerzenia Metamask oraz wysokiej znajomości funkcjonowania kryptowaluty Ethereum.

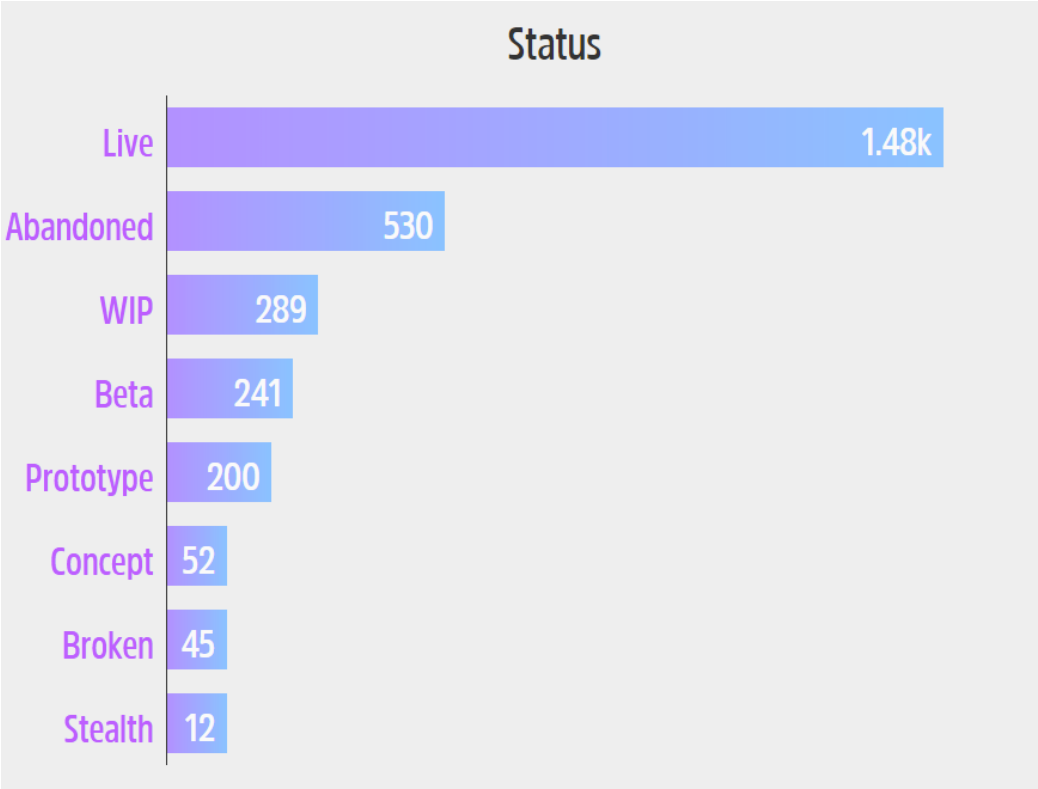
Platforms

Platform	Total DApps	Daily active users	Transactions (24hr)	Volume (24hr)	# of contracts
EOS	268	99.22k	1.36m	2.58m	370
Ethereum	2,473	18.83k	115.14k	35.54k	4.04k
Steem	76	13.56k	377.36k	255.31k	125
POA	18	1.05k	10.16k	11.4k	48
xDai	8	12	47	539	18
GoChain	4	2	6	0	15

Rysunek 13: dApps – statystyki

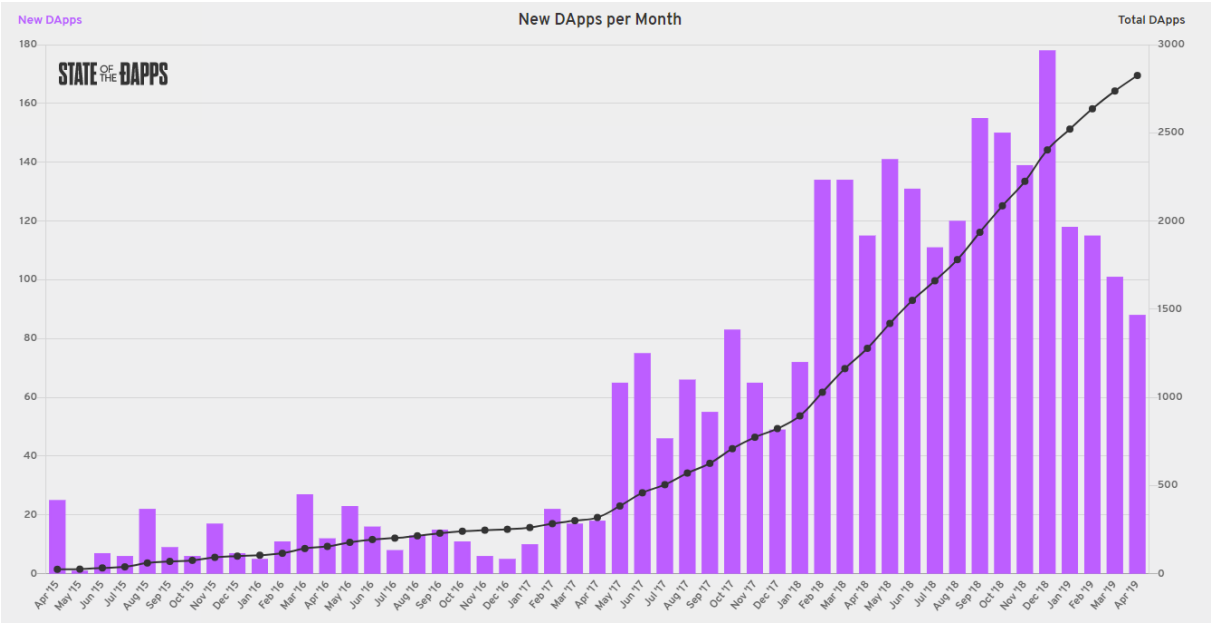
Największa liczba zdecentralizowanych aplikacji znajduje się na Ethereum. Jak możemy zauważyć, dAppsy na ETH przyciągają zaledwie 19 tysięcy użytkowników dziennie, razem tworzących wolumen w wysokości 36 tysięcy transakcji. Średnio więc, jeden aktywny użytkownik dApp generuje dwie transakcje w sieci Ethereum dziennie. Lepiej sytuacja przedstawia się na platformie EOS która, dzięki swoim popularnym kasynom, może pochwalić się 99 tysiącami użytkowników i wolumenem dziennym wynoszącym 2.5 miliona dolarów.

[14] https://www.stateofthedapps.com/rankings
[15] https://ylv.io/how-much-does-it-costs-to-run-dapp-in-2018/



Rysunek 14: Aktywne dApps

Jak możemy zauważyć, raptem niecałe 1.5 tysiąca z prawie 3 tysięcy dApp pozostaje aktywne. Jeżeli chodzi o zdecentralizowane aplikacje jesteśmy więc niezwykle wcześnie z tą technologią i dopiero przyszłe lata pokażą, czy zdoła ona przejąć część z rynku tradycyjnych aplikacji.



Rysunek 15: Wzrost ilości dApps

Deweloperzy zdają się nie ustępować w stworzeniu aplikacji, która osiągnie sukces jakim nie może się pochwalić obecnie żadna z dApp – **na przestrzeni ostatnich dwóch lat ilość dApp wzrasta wręcz wykładniczo.**

Możliwe perspektywy biznesowe dla technologii LISK

Czy LISK może okazać się lepszą platformą do dApps, aniżeli Ethereum lub EOS?

Jeżeli chcemy zdeponować dApp na łańcuchu głównym Ethereum, jedyne co musimy zrobić to przygotować kontrakt. Przy obecnych prowizjach pobieranych przez górników z transakcji, koszt założenia dApp na ETH wynosi ok. $15 USD[16]. Nawet jeżeli poziom zaawansowania naszej aplikacji wymagać będzie od nas zdeponowania kilku inteligentnych kontraktów, całościowy koszt nie powinien przekroczyć 0.3 ETH / $54 USD.

Zakładając, że nasz użytkownik korzysta z naszej aplikacji przez pół dnia w ciągu miesiąca, generując średnio 3 transakcje dziennie, dałoby to nam liczbę 1 080 000 transakcji w ciągu roku. Zatem koszt całościowy jaki użytkownicy musieliby pokryć za korzystanie z naszej dApp na ETH wyniósłby ok. $17100 USD rocznie.

EOS do założenia dApp wymaga RAMu. Koszt zdeponowania zdecentralizowanej aplikacji na EOS wynosi ok. $720 USD[17]. Lecz to nie wszystko. Deweloper dApp musi zapłacić za każdego nowego użytkownika swojej aplikacji. Przy 1000 użytkowników były to koszt ok. 10 000 EOS, czyli ponad $60000 USD[18].

Niestety, nie posiadamy jasnych danych odnośnie kosztów dApp na LISK. Whitepaper[19] mówi o koszcie 500 LSK za zdeponowanie dApp, niestety są to nieaktualne szacunki. Zakładając jednak, że byłyby prawdziwe, koszt dApp LSK, przy cenie $1.99 USD za LSK[20] wyniósłby $995 USD.

Koszt dApp LSK byłby zatem o 1842% większy od ETH i 38% większy od tej samej usługi na EOS. Pod uwagę nie są brane koszty operacyjne, a jedynie samo zdeponowanie dApp, gdyż nie

[16] https://ylv.io/how-much-does-it-costs-to-run-dapp-in-2018/
[17] https://ylv.io/how-much-does-it-costs-to-run-dapp-in-2018/
[18] https://www.eosrp.io/#calc
[19] https://github.com/slasheks/lisk-whitepaper/blob/development/LiskWhitepaper.md
[20] https://coinpaprika.com/waluta/lsk-lisk/

są znane koszty odpowiedniego zabezpieczenia i zapewnienia architektury serwerowej w przypadku sidechainów LISK.

Ostatnie propozycje deweloperów to ustanowienie ceny za dApps LISKa **na poziomie 25 LSK.** Dzięki temu mógłby on konkurować z EOS, lecz taki koszt nadal byłby wyższy o prawie 100% w porównaniu z ETH.

Jak więc możecie zauważyć, zarówno koszty jak i utrzymanie dApp jest obecnie potwornie drogie i zwyczajnie nieopłacalne w większości przypadków. Znacznie łatwiej jest zbudować klasyczną aplikację, która będzie tańsza i możliwa do łatwego wykorzystania przez potencjalnie miliardy ludzi na całym świecie. Dodatkowo korzystanie w tym celu z LISK jest zwyczajnie nie opłacalne pod względem ekonomicznym. Nie wiemy, czy zestaw narzędzi deweloperskich LISK SDK będzie oferował wystarczające benefity, które uczynią wyższy koszt deponowania dApp na LISK rozsądnym.

Na dzień dzisiejszy, LISK nie posiada nawet manualnie zdeponowanych sidechainów[21]. Nic nie wskazuje zatem na jakąkolwiek adopcję. Projekt GNY zapowiada w przyszłości migrację na platformę LISK.

Podsumowanie

Analiza wykazała, że koszty wiążące się z budową i zabezpieczaniem sidechainów przekraczają ich opłacalność jako narzędzie do budowania zdecentralizowanych aplikacji, w skrócie dApps. Rozwiązania proponowane przez Ethereum są tańsze, skuteczniejsze, bezpieczniejsze i posiadają znacznie większe wsparcie deweloperskie na całym globie.

Co więcej, rynek który LISK chce przejąć jest mikroskopijny, obrót kryptowalut wewnątrz dApps stanowi niewielki ułamek całościowego dziennego wolumenu transakcji. Nie istnieją również przesłanki świadczące o tym, że skala rynku dApps wzrośnie wykładniczo w najbliższym czasie, co pozwoliłoby LISKowi pozycjonować się jako konkurencja dla ETH i zawładnąć jedną z nisz. Kluczowy produkt LISK jakim jest SDK, pomimo okresu trzech lat, nie został wypuszczony na rynek nawet w formie niestabilnej wersji Alpha.

[21] https://www.liskdiscovery.com/sidechains

TOKENEKONOMIA

Według słów Maxa Kordka, LSK – natywna kryptowaluta sieci LISK jest w rzeczywistości tokenem użytkowym, za którego pomocą możemy płacić za różnego rodzaju transakcje występujące w LISK.

> We at Lisk don't believe in LSK being a currency, it's a utility token to empower the platforms users by utilising its features. That means, yes as you said it's a method to pay for the network fees which occur for different types of transactions.

Rysunek 16 Max Kordek - LSK token , Źródło: Reddit

Typy transakcji w obrębie blockchainu LISK[22]:

- Zwykły transfer służący do przesyłania środków między portfelami – opłata: 0.1 LSK
- Transakcja klasy: rejestracja dodatkowego hasła do portfela – opłata: 5 LSK
- Zarejestrowanie delegata – opłata: 25 LSK
- Głosowanie na delegatów – opłata: 1 LSK
- Multisygnaturowe zabezpieczenie konta – opłata: 5 LSK

Co, oprócz możliwości przeprowadzania kilku z powyżej wymienionych typów transakcji wewnątrz LISK sprawia, że token LSK zyskuje wartość? Cóż, według słów CEO – naprawdę niewiele:

> However, transactions on the mainchain are not the only use-cases for LSK. A sidechain is able to process LSK as well if the developer wants it. We at Lisk will definitely develop multiple Core Blockchain Apps like decentralised identity/storage/computation. They will very likely all run on LSK. Giving a custom token value and constant volume is hard, therefore I foresee some Blockchain Applications on Lisk will also simply use LSK, provided they don't need to conduct an ICO. If they need an ICO, then here we have another factor for demand. People will invest LSK into several ICOs being conducted on the Lisk platform.
>
> Out of the many points from above which give a token value, I have just discussed "purpose or use-case". There are also multiple other things we have not published yet, which will drive demand for LSK. There is more to come!

Rysunek 17: O wartości tokenu LSK - Źródło: Reddit

Kluczowym problemem z jakim borykają się wszystkie nowe kryptowaluty jest – jak nadać jej wartość. Jak sprawić, aby dana kryptowaluta nie tylko uważana była za wartościową poprzez zaufanie do projektu i czystą spekulację, lecz również posiadała rzeczywistą wartość. W

[22] https://lisk.io/help-center/getting-started/does-lisk-have-transaction-fees

przypadku Bitcoina wartość jest oczywista: Bitcoina jest gotówką internetu, rzeczywistym pieniądzem. Wokół niego zbudowana została ogromna infrastruktura giełd, kantorów, aplikacji, systemów itd. Cechy Bitcoina takie jak prywatność, wymienialność i uniwersalność tworzą jego wartość.

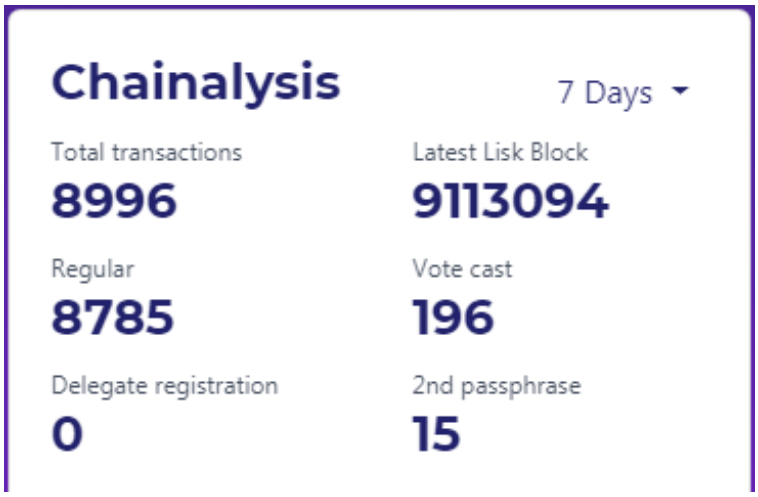
Jeżeli zakładamy, że głównym czynnikiem wzmacniającym popyt na daną kryptowalutę (popyt, nie jej wartość!) mają być przeprowadzone na danej platformie ICO, możemy niestety się przeliczyć (przypomnę, że w sekcji o sidechainach udowodniłem, że LISK nie jest obecnie zalecaną opcją do tworzenia dApps, a sidechainy zdecydowanie lepiej nadają się do kanałów płatności). Wydaje się, że właśnie taką sytuację obserwujemy obecnie w przypadku LISKa, co zamierzam potwierdzić analizą aktywności sieci.

Podsumowując token LSK służy do wysyłania i odbierania transakcji, głosowania, inwestowania w ICO na platformie LSK i handlu na giełdach. Poza tymi cechami, nie posiada na ten moment żadnych innych zastosowań. Deweloperzy zdają się nie mieć jasnego planu który miałby zwiększyć wartość LSK. Przykład aktywności sieci pokaże, że nie można w tym celu liczyć na zwiększoną adopcję. Nawet w przypadku już aktywnych sidechainów LISK, wykorzystują one własne tokeny, a nie LSK.

Aktywność sieci LISK

Do celów tego raportu, przy pomocy publicznie dostępnych danych, przeprowadziłem analizę blockchainu LISK i rzeczywistego wykorzystania sieci, aby określić stopień adopcji oraz zaangażowania deweloperów i społeczności.

Każdego dnia wpada 8640 bloków w blockchainie LSK. Całkowita tygodniowa liczba transakcji wynosi zaledwie 8996. Oznacza to, że średnio co 6.72 bloków sieć LISK przetwarza jedną transakcję. Czyli otrzymujemy liczbę średnio 0.15 transakcji na blok. Co minutę i 10 sekund blockchain LISK przetwarza jedną transakcję.

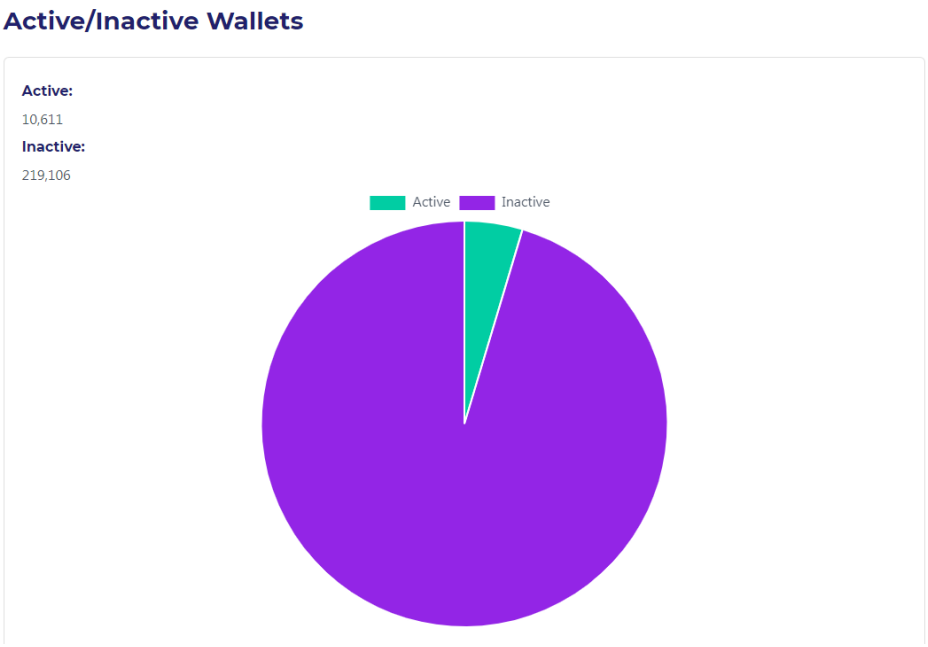


Rysunek 17: Źródło: Lisk Chainalysis

Przez rok, delegaci poprzez „forging" wytworzyli prawie 11 mln LSK, utrzymując tym samym inflacje roczną LSK na poziomie ok. 11%. Zforgowane coiny stanowiły ponad 10% ogólnej podaży LSK:

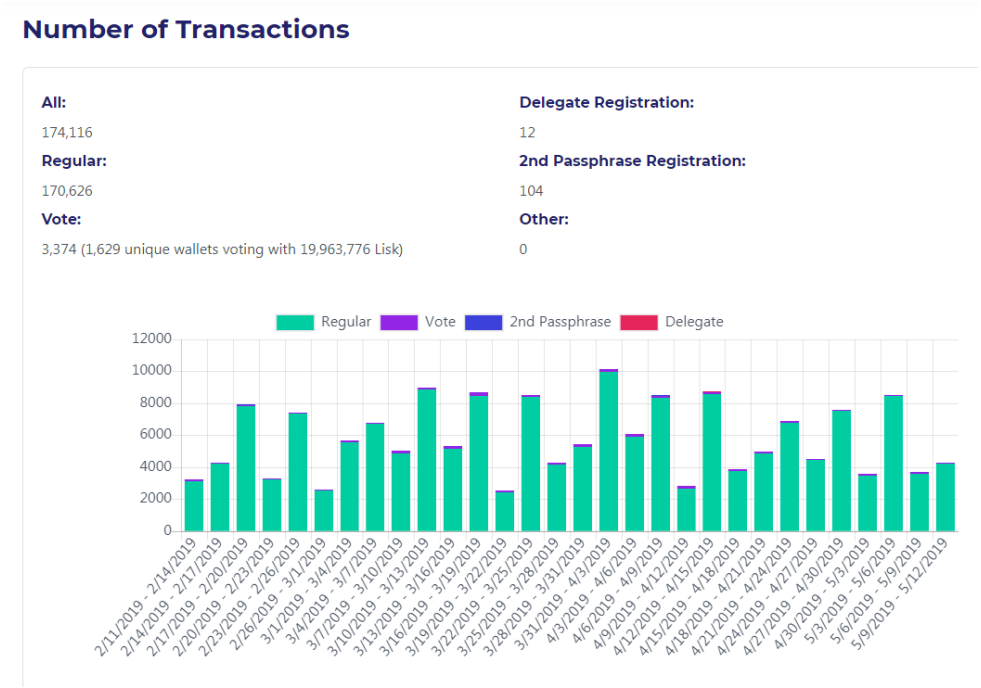
Rysunek 18: Źródło: Chainalysis

Badanie aktywności portfeli wykazało, że raptem 5% wszystkich walletów było aktywnych w ciągu ostatnich 3 miesięcy:



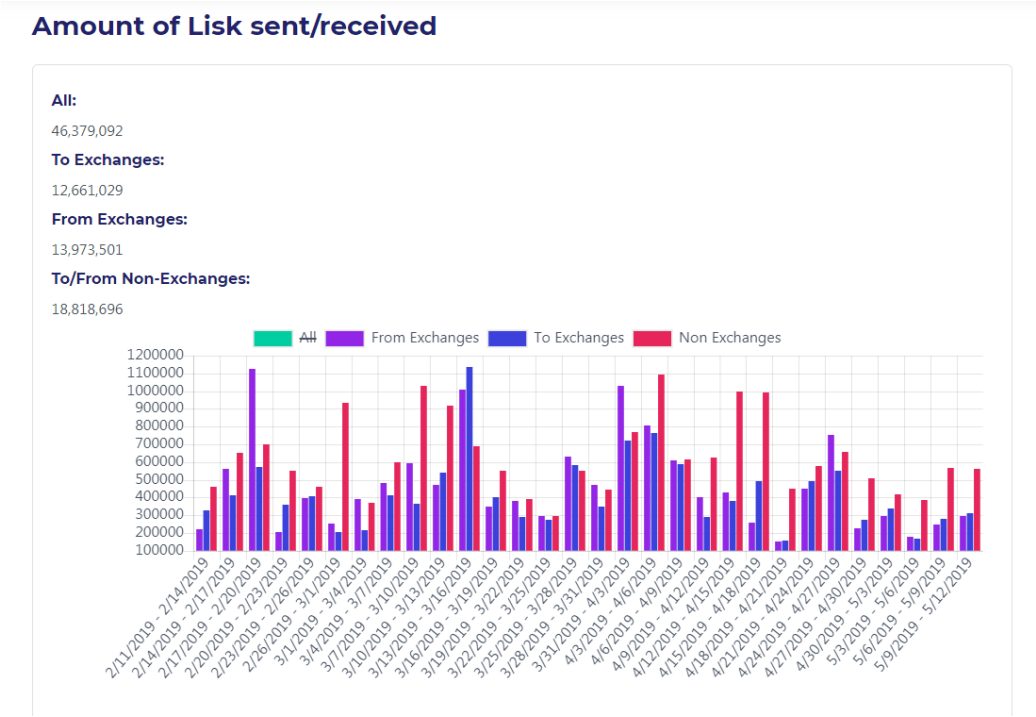
Rysunek 19: Aktywność portfeli LSK

W ciągu trzech ostatnich miesięcy, delegaci przetworzyli 174 tyś transakcji. Dla porównania, sieć BTC dziennie potwierdza średnio 350 tyś transakcji.



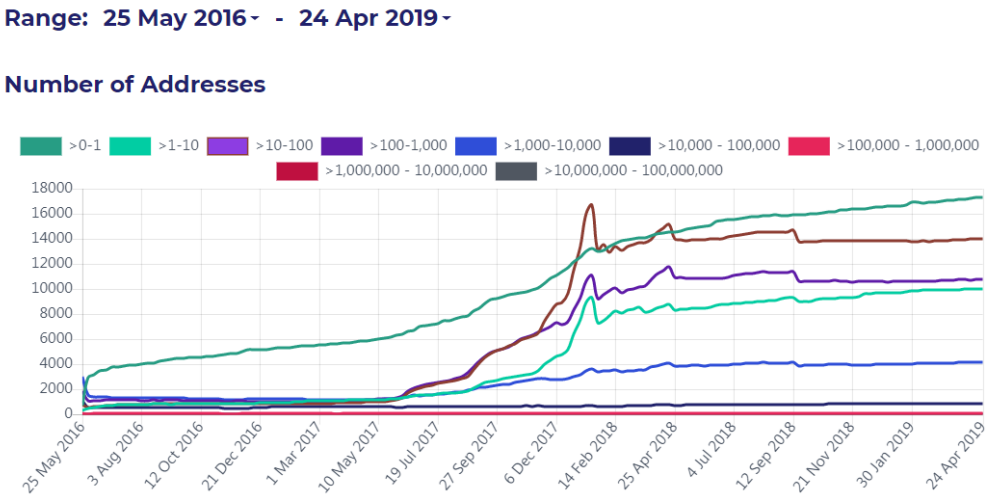
Rysunek 20: Liczba transakcji LSK - 3 miesiące

Liczba przesłanych w tym czasie LSK wynosi 46 mln i stanowi ok. 38.5% całości podaży tokenu LSK.



Rysunek 21: Liczba przesłanych LSK

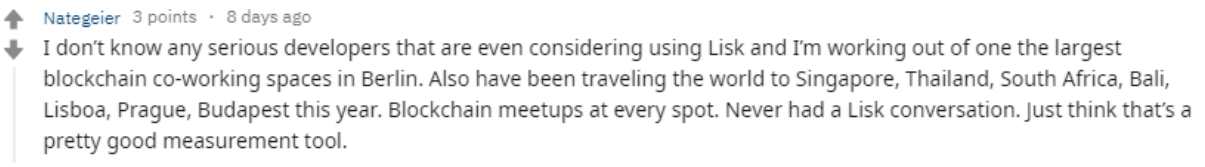
LISK posiada 16 tysięcy adresów. Na poniższym wykresie możemy zobaczyć jak zmienia się ich ilość od początku powstania LISK czyli 2016 roku.



Rysunek 22: Liczba adresów LISK

Token LSK dostępny jest obecnie na giełdach w 56 parach i jedynie 15 z nich posiada odpowiednią płynność do jakiegokolwiek handlu[23]. Według raportu instytutu BTI, 38% z dziennego wolumenu LISK jest wash-tradeowane[24]. Przy czym przypominam, że nie jest to wina deweloperów, ani projektu, lecz nieuczciwych giełd.

Sprawdzając sentyment inwestorów posiadających tokeny LSK, natrafiłem na ciekawe stwierdzenie jednego z nich:


Nategeier 3 points · 8 days ago

I don't know any serious developers that are even considering using Lisk and I'm working out of one the largest blockchain co-working spaces in Berlin. Also have been traveling the world to Singapore, Thailand, South Africa, Bali, Lisboa, Prague, Budapest this year. Blockchain meetups at every spot. Never had a Lisk conversation. Just think that's a pretty good measurement tool.

Rysunek 23: Źródło: Reddit

Wnioski:

- Sieć LSK posiada znikomą aktywność
- Blockchain LISK jest praktycznie nieużywany
- Ogólna liczba przetworzonych transakcji, w porównaniu do reklamowanej skali projektu, jest bardzo mała
- Token LSK wykorzystywany jest w większości do handlu na giełdach i spekulacji
- 95% portfeli LISK pozostała nieaktywna w przeciągu ostatnich 3 miesięcy

DPOS – Demokratyczny model delegatów LISK

Zacznijmy od fundamentalnej sprawy dotyczących protokołów konsensusu – inicjatywy ekonomicznej dla węzłów w celu bezstronnego zachęcania ich do wykorzystywania swoich zasobów do zabezpieczania sieci. Z pozoru wydawałoby się, że LISK i Bitcoin niewiele się pod tym względem różnią i oba z nich oferują ciekawy model ekonomiczny. Jeśli rozważamy jednak inicjatywę ekonomiczną w przypadku dPOS i POW są one jednak wyraźne różne.

[23] https://coinmarketcap.com/currencies/lisk/#markets
[24] https://www.liskmagazine.com/blog/2019/04/19/38-of-fake-trading-volume-on-lisk-according-to-bti-april-report/

W celu lepszej wizualizacji stwórzmy prosty eksperyment myślowy. W pierwszej kolejności ustanowimy dwa różne modele, z dwoma różnymi zasadami początkowymi. Jeden model obrazował będzie blockchain oparty o konsensus dPOS, drugi natomiast odzwierciedla system jaki znamy z POW. Rozważmy w takim razie czynnik zaufania i bezpieczeństwa sieci, mając na uwadze, że dążymy do sytuacji w której sieć byłaby jak najbardziej niezależna od pojedynczych uczestników, zdecentralizowana i przez to zwiększone byłoby jej bezpieczeństwo. Ważne jest również, aby zauważyć, że potrzebujemy wyraźnej inicjatywy ekonomicznej która umożliwiłaby sprawiłaby, że ewentualnym węzłom/górnikom/delegatom (nie ważne jak nazwiemy osoby odpowiedzialne za utrzymanie sieci, walidowanie transakcji itd.) **opłacałoby** się poświęcać zewnętrzne zasoby w celu uczestnictwa w sieci.

W przypadku naszego pierwszego modelu opartego na dPOS, taką inicjatywą jest inflacja.

Drugi model, który opiera globalne porozumienie na protokole POW, wynagradza górników określoną ilością jednostki kryptowaluty (np. w sieci Bitcoin jest to BTC) za rozwiązywanie kryptograficznych puzzli, czym zabezpieczają blockchain. Górnicy, swoją mocą obliczeniową, transmitują również transakcje użytkowników.

Na pierwszy rzut oka kilkuprocentowa inflacja w modelu nr. 1 nie różni się niczym od otrzymywania wydobytych jednostek kryptowaluty w modelu nr. 2. Początkowa inicjatywa w obu modelach jest jasna i podobna. Różnice uwypuklają się jednak kiedy pozwolimy naszemu systemowi działać. Czas w tym wypadku, powoduje znaczące różnice w funkcjonowaniu obu systemów i choć aplikujemy podobne reguły startowe, wynik końcowy jest znacząco różny.

Jeszcze jedną ważną rzeczą jaką musimy założyć jest to, że potencjalny uczestnik naszego modelu jest całkowicie egoistyczny – co znaczy, że wkładając w model określony zasób pracy, oczekuje jak największych zysków dla siebie.

W modelu dPOS kluczową rolę dla potencjalnego egoistycznego uczestnika, pragnącego zyskać z uczestnictwa w sieci jak najwięcej dla siebie, odgrywa „gromadzenie”. Znamy początkowe reguły gry – im więcej kryptowaluty zgromadzisz, tym większą wagę ma twój głos, który z kolei pozwala ci głosować nad przyszłym stanem sieci. W najlepszym wypadku, chciałbyś zachować jak najwięcej wpływu na sieć i władzy w swoich rękach – jak więc powinieneś się zachowywać, aby odzwierciedlać tą idee? Gromadzić tyle kryptowaluty w swoich własnych rękach ile tylko się da. Spowoduje to, że jeśli do gry będą chcieli dołączyć nowi uczestnicy, zasób kryptowaluty która im na to pozwala, będzie w znacznej części w twoich rękach.

Mamy więc mniej więcej przedstawione zachowanie potencjalnego uczestnika sieci pragnącego egoistycznie (egoistyczne zachowanie jest w tym wypadku jedyną opcją) zyskać jak najwięcej. Teraz powiększmy nasz model do 101 uczestników walczących między sobą o wpływy i inflacyjny zasób kryptowaluty. Pamiętajcie, każdy z nich walczy o kontrolę nad

zasobem danego „surowca”, gdyż to on pozwala jemu utrzymać się u władzy i czerpać z sieci jak największe dochody. Co zatem otrzymamy?

Uproszczony model ekonomiczny funkcjonowania sieci LISK.

Gdy delegaci LSK zgromadzą już określoną liczbę kryptowaluty zapewniającą im miejsce na szczycie hierarchi delegatów, wątpliwe jest, aby danym zasobem chcieliby się podzielić. Dla potencjalnego nowego delegata, nawet zakładając jego uczciwe motywy i chęć zwiększenia zaufania sieci poprzez swoją kandydaturę, ciężkie jest zebranie wymaganej do złamania hegemonii liczby LSK, gdyż są one posiadane przez obecnych delegatów. Nie ma więc dostępu do wystarczającego zasobu kryptowaluty, gdyż jest on w całości kontrolowany przez aktualnych delegatów.

W przypadku kopania Bitcoina, mamy do czynienia z mocą obliczeniową, jest więc to kompletnie niezależny od samego Bitcoina surowiec. Nie ważne więc jak wielką moc obliczeniową posiada dany górnik lub stowarzyszenie górników, nawet gdyby doprowadziło do uzyskania monopolu posiadając większość mocy obliczeniowej, w grze może pojawić się nowy uczestnik, posiadający moc obliczeniową z zewnątrz, gdyż jej zasób nie jest zależny od samej sieci Bitcoin.

Moc obliczeniowa jest zatem surowcem zewnętrznym i niezależnym od samego BTC! Gromadzenie BTC na nic się nie sprawdza w POW. Nie istnieje inicjatywa ekonomiczna do gromadzenia BTC, a potencjalny górnik powinien pozbyć się BTC, w celu uzyskania zysku (odliczając koszty mocy obliczeniowej).

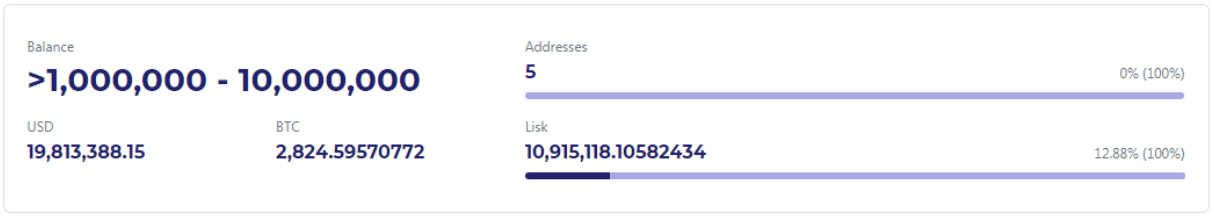
Tak, jeśli wierzysz w rozrost projektu i większą adopcję w przyszłości, gromadzenie BTC ma sens ekonomiczny, jednak jest to zupełnie inny czynnik, nie wynikający z reguł początkowych systemu!

W przypadku LSK jest natomiast odwrotnie. Im dłużej jakiś delegat pozostaje na stanowisku, tym więcej LSK posiada, tym mniejszy jest ich zasób dla potencjalnych nowych kandydatów. Jedyne więc spory mogą występować w obrębie poszczególnych grup już aktywnych delegatów, w celu uzyskania jeszcze większej kontroli nad zasobem LSK. Wydaje się, że właśnie taką sytuację obserwujemy z grupami GDT, Elite i Sherwood.

Gromadząc LSK zyskujesz władzę w systemie. Nie istnieje również żaden zewnętrzny „surowiec” (tak jak w przypadku mocy obliczeniowej w Bitcoinie która jest niezależna od

naszego systemu) który mógłby zostać wykorzystany do pozbawienia cię władzy. Może to zrobić jedynie kolektyw, grupa równie silnych delegatów, która dzięki połączonym siłom, zyskuje większą władzę w systemie od ciebie.

Spójrzmy teraz czy naszą hipotezę potwierdzają dane z blockchain. Ze zbioru danych wykluczone zostały portfele zespołu LISK oraz giełd.



Rysunek 24: Liczba adresów posiadających powyżej miliona LSK

Rysunek 25: Liczba adresów posiadająca ponad 100 tyś LSK

Prawie $40 mln LSK przetrzymywanych jest przez 154 adresy LSK. Liczba adresów z taką ilością LSK (patrz wykres w sekcji o aktywności sieci) nie ulega zmianie w czasie. Zatem od początku mniej więcej równa ilość adresów posiada znaczny zasób tokenów LSK. Biorąc pod uwagę, że aktywność portfeli plasuje się na poziomie 5%, adresy te mają znaczną przewagę w procesie demokratycznego głosowania na delegatów i mogą utrzymać swoją hegemonię jeśli nie dojdzie między nimi do wewnętrznych walk.

W przypadku LISK często można usłyszeć o „kartelach” – określa się tak monopol na „demokracje” poszczególnych grup delegatów. Uważam, że określenie karteli jest nietrafione i krzywdzące. Deweloperzy LISK ustalili określone reguły systemu, a kiedy użytkownicy zaczęli z niego korzystać, ekonomia i wolny rynek sprawiły, że obserwujemy obecnie sytuację, w której to niezwykle ciężko jest przełamać monopol grup delegatów bez fundamentalnej reorganizacji sieci. Jest to tylko i wyłącznie wina deweloperów LISK, którzy ustalili reguły gry.

Niepokój dotyczący karteli obrazują liczne źródła[25][26][27][28]. Deweloperzy LISK zaczęli podejmować kroki w celu zmiany tego stanu rzeczy[29].

Sprawa delegatów jest ważna jednak pamiętajmy, że model ten stanowi jedynie sposób dojścia do globalnego konsensusu który wykorzystuje LISK**. DPOS nie jest zatem sam w sobie jakimkolwiek plusem bądź minusem dla ogólnego postrzegania projektu.** Jest tylko narzędziem wykorzystanym do osiągnięcia danego celu – potwierdzenia, że środki przechowywane na portfelu LISK są rzeczywiście Twoje i nikt inny nie jest w stanie ich wykorzystać. Delegaci, choć jest to niezmiernie ciekawy system, nie są więc atutem Liska, czymś co przyciągnąć ma deweloperów lub doprowadzić do szerszej adopcji.

Chciałbym przedstawić jeszcze jedną obserwację na temat systemu DPOS oraz demokracji w blockchainie.

Zaufanie i delegaci

Trywialnym byłoby zakładać, że użytkownicy sieci zawsze będą wybierać najuczciwszych i rzetelnych delegatów. Dlaczego?

Role i obowiązki delegatów:

- *Zapewnienie, że ich węzeł jest zawsze aktywny*
- *Propagowanie bloków*
- *Podpisywanie i nadawanie tych bloków, walidacja transakcji.*
- *W przypadku problemów z konsensusem sieciowym, rozwiązanie go poprzez mechanizm głosowania*

1. Delegaci również są użytkownikami, w których inicjatywie jest posiadanie jak największej ilości kryptowaluty.

[25] https://medium.com/coinmonks/lisk-the-mafia-blockchain-47248915ae2f

[26] https://www.reddit.com/r/Lisk/comments/8c1r5m/lisk_cartel/

[27] https://captainaltcoin.com/crypto-projects-with-no-future-elite-cartel-dominated-dapp-platform-lisk-lsk/

[28] https://blog.goodaudience.com/the-time-for-independent-lisk-delegates-has-come-2e70db451319

[29] https://captainaltcoin.com/lisk-lsk-about-to-dismantle-delegate-cartels-new-roadmap-is-out/

2. Głosujący mogą nie posiadać kompletnych informacji o sprawowaniu się danego delegata w sieci.

3. Głosujący mogą zwyczajnie nie dbać o jak najlepszy stan sieci, a na przykład inną inicjatywę ekonomiczną, zapewnioną np. przez nieuczciwego delegata.

4. Głosujący mogą zwyczajnie nie dbać o sieć – nie dokładając należytych starań w celu określenia który z delegatów stanowi najlepszą opcję dla bezpieczeństwa sieci, która z kolei przekłada się na bezpieczeństwo własnych jednostek kryptowaluty głosującego.

Pragnę również dodać, że głosowanie staje się opłacalne dopiero w momencie posiadania przynajmniej 1000 LSK. Możemy wtedy liczyć na (minus opłata za głosowanie) 7-8 LSK miesięcznie, czyli ok. 60 PLN pasywnego dochodu miesięcznego. Uwzględniając roczną inflację na aktualnym poziomie ok. 11%, z naszych bonusowych środków niewiele się ostaje. Inicjatywa ekonomiczna do głosowania jest zatem niewielka.

Hacki i bugi sieci LISK

Blockchain LISK nigdy nie został zhackowany, a środki nie zostały skradzione. Zdarzały się jednak przypadki poważnych błędów. Największym z nich było zatrzymanie i całkowity paraliż blockchainu LISK na 12h[30]. Temat na platformie Reddit, w którym ogłosił to CEO Max Kordek został usunięty[3132], jednak zachowało się archiwum z tego wydarzenia, w poście opublikowanym na forum.bitcoin.pl (patrz przypis nr. 30).

[30] https://forum.bitcoin.pl/viewtopic.php?t=21652&start=13720

[31] https://www.reddit.com/r/Lisk/comments/8o033l//?utm_content=body&utm_medium=post_embed&utm_name=ee1aeb0dde72406bb54888194697d1ab&utm_source=embedly&utm_term=8o033l

[32] https://www.reddit.com/r/Lisk/comments/8o73ap//?utm_content=body&utm_medium=post_embed&utm_name=8afecac244284f99b8ed2b8d62e5f645&utm_source=embedly&utm_term=8o73ap

Lisk Blockchain Temporarily Halts Due to an Automated Security Measure - All Funds Safe and Fix Implemente

Dodane 1 dzień temu przez MaxKK President & CEO

During European morning hours, an anonymous individual broadcasted a faulty transaction to the Lisk network. Due to a rare edge-case bug in transaction processing, this transaction was deemed valid and went through the processing steps on each individual node. However, it was an invalid, maliciously customized transaction type that utilised this particular code bug.

For these cases there are security measurements built into Lisk Core in order to prevent the blockchain from continuing and causing forks. For this reason every individual node has temporarily stopped processing new blocks which has resulted in the Lisk network to halt. This is automated and intended behaviour in order to protect our users from any loss of funds.

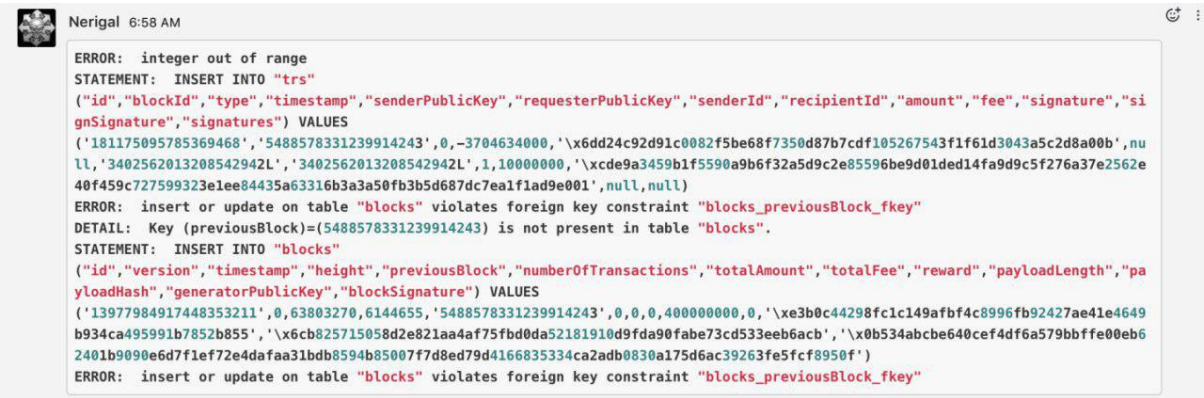
At this time, there are currently 150 transactions in limbo which occurred after the incident, but were never included into the Lisk blockchain. Our current plan is to not re-broadcast these transactions. The network will continue as if these transactions have never happened - this means no funds are at risk.

In lieu with our commitment to full transparency, we have had similar edge-cases take place 2 or 3 times in the past. In all scenarios, the Lisk blockchain always remained secure, as intended, through the deployment of new Lisk Core versions which fixed such issues and allowed for the Lisk blockchain to continue running as normal.

The fix for this matter has already been discovered and implemented. Today, we will release Lisk Core v.0.9.15 which will resolve the issues and allow for the continual and normal operation of the Lisk network. When this fix is deployed we will ask for all delegates to rebuild their nodes by upgrading to the newest version. Further updates to our community will take place as we progress with resolving this issue.

Rysunek 26: Oświadczenie Maxa Kordka na Reddicie

Problem polegał na tym, że blockchain LISK nie potrafił procesować liczb ujemnych i kiedy takowe zostały do niego wprowadzone, sieć ulegała awarii. Sytuacja miała miejsce w 2017 roku.



Rysunek 27: Blockchain LISK nie akceptował liczb ujemnych

Podsumowanie analizy kryptowaluty LISK

Jakkolwiek nie wychwalałbym LISKa za świetny design i niesamowicie przygotowaną Lisk Academy, nie przykryje to braku jakiegokolwiek produktu oraz bardzo niskiej aktywności sieci. Nie sposób również ukryć niedotrzymanych terminów i problemu ze zbyt silnymi grupami delegatów. Do mankamentów projektu zaliczyć możemy również niedostosowanie technologii do problemu – jak wykazała analiza, sidechainy nie są obecnie optymalnym rozwiązaniem problemu skalowalności. Koszty ich założenia skutecznie uniemożliwiają wykorzystanie ich w celu budowy zdecentralizowanych aplikacji, co potwierdza brak adopcji LISKa pomimo kilku lat rozwoju projektu.

stokarz

Archiwum raportów:

https://ambrosus.pl/latwe-wejscie-w-blockchain-amb-net-masternode-system/ - Ambrosus (AMB)

https://www.docdroid.net/bmUvPow/neo-raport-by-stokarz.pdf - NEO

https://www.docdroid.net/WS10r86/stellar-konsensus-raport-by-stokarz.pdf - Stellar (XLM)

Jeżeli interesuje Cię technologia kryptowalut, moje artykuły znajdziesz na portalach:

https://ambrosus.pl/

https://cyberkrypto.pl/

Kanały na platformie Telegram na których się udzielam (@stokarz):

https://t.me/ArcyTradeAltyczat

https://t.me/arcytradebitmexczat

https://t.me/CyberKryptoFreedomChat