Czerwiec 2019

ETH 2.0 – RAPORT

Przecierając szklaki ku

zdecentralizowanej przyszłości

Autor: stokarz

Raport powstał dzięki współpracy i zaangażowaniu grupy CyberKrypto. Jeżeli dopiero zaczynasz swoją przygodę z kryptowalutami, CyberKrypto jest świetnym miejscem do rozpoczęcia nauki i zasięgnięcia rad od prawdziwych weteranów kryptowalut.

Podziękowania również dla Tomasza Drwięgi z Parity, za sprawdzenie raportu i poprawę wszelkich błędów merytorycznych.

Decentralizacja jest potężnym hasłem. Choć obserwując naturę ciężko jest dojrzeć schematy funkcjonowania, którym moglibyśmy nadać miano zdecentralizowanych, okazuje się, że taka forma działania ma niezwykłe właściwości w wielkoskalowych systemach. Uwidacznia się to szczególnie w przypadku gromad ludzkich, a także technologii przez nas tworzonej. Zastąpienie hierarchicznej struktury zarządzania, jej zdecentralizowaną wersją – rozproszenie zasobów, decyzyjności i wreszcie władzy, sprawia, że takowe systemy zyskują unikatowe cechy: brak możliwości wprowadzenia niechcianych zmian, poprzez jedną, złośliwą organizację, wysokie bezpieczeństwo wynikające z potrzeby przeprowadzenia ataku na zdecentralizowaną infrastrukturę, czy równość szans, bez względu na pochodzenie, rasę, płeć lub inne ludzkie cechy. Przydają się one w środowisku, w którym przykładowy uczestnik nie może okazać zaufania. Z różnych powodów. Być może pragnie zachować anonimowość, gdyż jego prawdziwa tożsamość zdradziłaby, że jest zbiegiem politycznym, tym samym eliminując go z uczestnictwa.

Ostatnie dziesięć lat, czas w którym powstał i skutecznie działał Bitcoin pokazały, że zdecentralizowane systemy świetnie nadają się do finansów. Pomimo że, próby stworzenia wolnego, równego i bezpiecznego cyfrowego pieniądza trwały od początku lat 90, dopiero zastosowanie przez Satoshiego Nakamoto czynnika decentralizacji i drastyczne ograniczenie potrzeby indywidualnego zaufania sprawiły, że globalna oraz otwarta sieć informacji jaką jest Internet, ciągle rosnący w siłę i zmieniający drastycznie nasze życia, otrzymał narzędzie służące do wymiany wartości wewnątrz niego. Co z pozoru może wydawać się błahostką, stanowiło kamień węgielny pod nowego rodzaju ekonomię. Pierwsze jej kroki jesteśmy w stanie obserwować już dziś, a rozkwit zobaczymy w ciągu następnej dekady.

Aby lepiej zrozumieć fenomen kryptowalut, musimy cofnąć się o tysiące lat wstecz i objąć naszym postrzeganiem o wiele szerszy horyzont wydarzeń. Odkąd nasze mózgi stały się na tyle potężne żeby zrozumieć ideę transakcji między osobnikami tego samego gatunku – w tym wypadku homo sapiens – często pragnęliśmy posiadania przedmiotów i dóbr naszego „sąsiada” z plemienia. Jak jednak wymienić owoce mojej własnej pracy, na przedmiot stworzony przez kogoś innego? Wprowadzenie uniwersalnego miernika abstrakcyjnej wartości, możliwość wyceny towarów, a później usług, stanowił dla ludzkości osiągnięcie na miarę odkrycia ognia. Z momentem wymiany pierwszej muszli kauri, służącej dawnym osadom ludzkim jako waluta, na towar, rozpoczął się proces formowania tego, co dziś nazywamy nowoczesną ekonomią. Unifikacja miar wartości, ten swoisty niepisany kontrakt społeczny, była przyczyną naszego globalnego rozwoju.

Wiemy już zatem, jak potężnym narzędziem jest pieniądz i jaką rolę odgrywał w naszej historii. Przyjrzymy się teraz czasom współczesnym.

Drastyczny rozwój internetu jaki przypada na lata 90 XX wieku do czasów współczesnych, uwidacznia niezwykły wręcz skok szybkości dokonywanego przez ludzkość postępu. Jednak dotychczas internet był znacznie ograniczony. Pozwalał nam na transmitowanie informacji, jednak przesyłanie wartości nadal pozostawało w rękach tradycyjnego systemu finansowego, wraz ze scentralizowanymi instytucjami, które od dziesiątek lat dzierżą nad pieniądzem pełnię władzy. Nawet usługi takie jak Paypal lub nowoczesne systemy płatności online od Mastercard, nadal pozostawały w rękach jednego centralnego organu. Organu, który posiada możliwość ingerencji w finanse – cofnięcia transakcji, jeśli jest ona niezgodna z polityką firmy lub cenzorowania osób pochodzących z określonych krajów. Internetowi potrzebne było narzędzie, które sprawi, że wartość – pieniądz, przesyłać można będzie anonimowo, demokratycznie, a ludzie obsługujący sieć posiadać będą jasną inicjatywę ekonomiczną dla przysłania transakcji – nie ważne jakiego są pochodzenia.

I tym właśnie jest Bitcoin. Pieniądzem dla Internetu.

Rozwój i innowacyjność nie lubi jednak zastoju. Bitcoin był, jest i nadal będzie świetnym cyfrowym pieniądzem, z którego korzystać może każda osoba na Ziemi. Lecz Bitcoin jest aż pieniądzem i tylko pieniądzem. Tak został zaprogramowany i to zadanie spełnia. Szybko jednak okazało się, że Bitcoin otworzył wrota do nowej gałęzi nauki, jaką są, ogólnie - kryptowaluty. Będąc na styku dziedzin ekonomii, informatyki, matematyki, psychologii rynkowej, systemów rozproszonych – interdyscyplinarne – wynalazcy tego świata bardzo szybko doszli do, trafnych zresztą, wniosków, że technologię znaną z Bitcoin zastosować możemy do innych problemów.

Tak właśnie, w 2014 roku, z inicjatywy Vitalika Buterina powstało Ethereum (ETH). Ethereum to publiczna, rozproszona platforma obliczeniowa wykorzystująca blockchain, posiadająca możliwość tworzenia smart kontraktów i zdecentralizowanych aplikacji – dApp. Wyceniany dziś na 26 miliardów USD i przetwarzający dziennie 900 tys. transakcji projekt, czekają ogromne zmiany będące wynikiem pięciu lat badań i testów. Druga wersja Ethereum, nazywana po prostu ETH 2.0 wniesie do kryptowaluty mnóstwo udoskonaleń technicznych, które mają przyśpieszyć sieć, zwiększyć potencjalną skalowalność i pozwolić Ethereum na stanie się rzeczywistym globalnym komputerem.

W tym raporcie przyjrzymy się nadchodzącej aktualizacji ETH 2.0, rozważymy jej mocne i słabe strony, konsekwencje, a także potencjalne zagrożenia. Przyjrzymy się realnym zastosowaniom Ethereum, skali adopcji i rosnącej, z dnia na dzień, konkurencji rynkowej.

Zapraszam w podróż ku zdecentralizowanej przyszłości. stokarz

O autorze

Zajmuję się analizą i badaniem rynku oraz technologii kryptowalut. Raporty mojego autorstwa mają charakter prywatnej opinii i nie stanowią porad inwestycyjnych. **Wykonuję analizy dowolnych kryptowalut na zlecenie**, a także angażuję się w różnego rodzaju projekty z dziedziny kryptowalut.

W celach współpracy proszę o kontakt:

E-mail: stokarzlol@gmail.com

Telegram: @stokarz

Kluczowe wnioski raportu:

- ETH 2.0 – Serenity sprawi, że Ethereum stanie się szybsze, a sieć zyska większą przepustowość, przy jednoczesnym zwiększeniu decentralizacji i wynikającego z niej wysokiego poziomu bezpieczeństwa.
- Serenity wprowadzi w Ethereum technologie takie jak: Casper, Sharding i eWASM.
- Plasma i State Channels umożliwią Ethereum skalowanie off-chain (poza łańcuchem głównym).
- ZK-STARKS i Zether pozwolą na wprowadzenie do Ethereum cech prywatności znanych z Zcash i Monero.
- Ethereum posiada największą grupę aktywnych deweloperów ze wszystkich podobnych kryptowalut.
- Nie istnieją obecnie jasne przesłanki wskazujące na potencjalne zajęcie miejsca Ethereum przez jakąkolwiek z podobnych kryptowalut z dziedziny smart kontraktów i zdecentralizowanych aplikacji.
- Należy wziąć pod uwagę, że pełne wprowadzenie Serenity zajmie przynajmniej 3 lata.
- Ethereum narażone jest również na kilka poważnych, potencjalnych zagrożeń – wysoka inflacja, sabotowanie protokołu przez górników lub niemożność wprowadzenia zakładanych technologii w rzeczywiste środowisko sieciowe.

Ogólna ocena projektu:

8/10

Ethereum

Celem tego raportu nie jest wprowadzenie do kryptowaluty jaką jest Ethereum, a określenie jej aktualnego potencjału, przyszłego możliwego wzrostu lub spadku na znaczeniu na tle rynku oraz przedstawienie danych, jakie dostarcza nam badanie aktywności publicznego blockchaina ETH. Czytelnikowi, który nie miał jeszcze większej styczności z kryptowalutami, zalecam wpierw zapoznanie się z fundamentami Ethereum, a dopiero później przeczytanie raportu. Internet pełny jest świetnych opracowań o podstawach ETH.

Ogólny konsensus społeczności kryptowalutowej zakłada, że całkowita kapitalizacja danego aktywa jest na razie jednym z najlepszych mierników jego znaczenia, a także adopcji. Ethereum (ETH) zajmuje obecnie zaszczytne drugie (2) miejsce na listach całkowitej kapitalizacji, będąc wycenianie na 26 miliardów USD, przy cenie 256 USD[1] za sztukę. Realny dzienny wolumen wynosi 334 mln USD, według danych OnchainFX[2]. Instrumenty pochodne oparte o ETH, w szczególności produkt ETH Quanto Perpetual od Bitmex, pozostają drugimi najchętniej tradeowanymi instrumentemi na rynku kryptowalut. Ich wolumen dzienny wynosi 366 mln USD[3]. Dane te obrazują niemalejące zainteresowanie kryptowalutą Ethereum od strony rynkowej.

Sieć Ethereum funkcjonuje w oparciu o protokół POW (Dowód Wykonanej Pracy), w której to górnicy walidują transakcje, czerpiąc z tego korzyść ekonomiczną w postaci nagród z bloków. Średnia nagroda z bloku wynosi 2.1 ETH[4]. Dziennie wydobywanych jest 5 900 bloków, co daje nam 20 296 ETH. Oprócz opłat transakcyjnych, dzienny przychód górników wynosi ok. 5 mln USD (nie uwzględniając kosztów sprzętu). Dane te mają szczególne znaczenie w kontekście planowanej migracji z protokołu POW na wydajniejsze POS i wyeliminowanie górników z łańcuchu ETH, co omówimy w dalszym rozdziale.

---

[1] Coinpaprika ETH data:
https://coinpaprika.com/

[2] OnchainFX Real Daily Volume. *OnchainFX w swojej analizie uwzględnia jedynie wolumen pochodzący z 10 największych i najbardziej zaufanych giełd, nie stosujących praktyk wash-tradeingu*:
https://messari.io/onchainfx

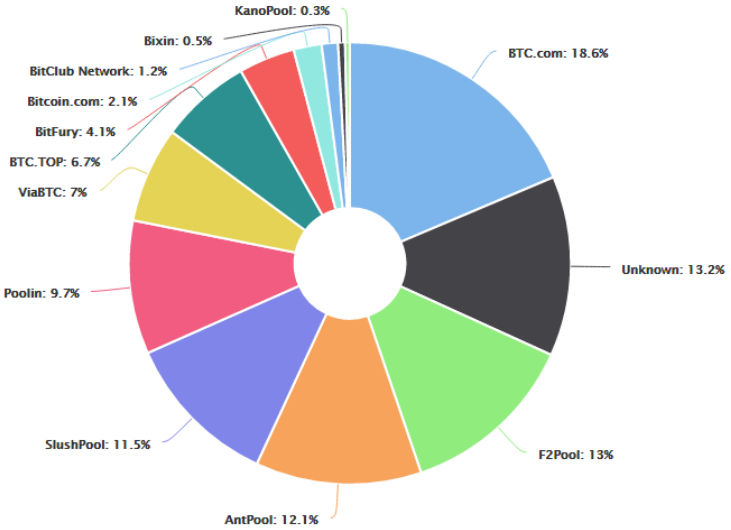
[3] BraveNewCoin ETH Quanto 24h Bitmex data:
https://bravenewcoin.com/data-and-charts/exchanges/169/markets

[4] Vlad Zamfir. Against Vitaliks fixed supply eip.
https://medium.com/@Vlad_Zamfir/against-vitaliks-fixed-supply-eip-eip-960-18e182a7e5bd

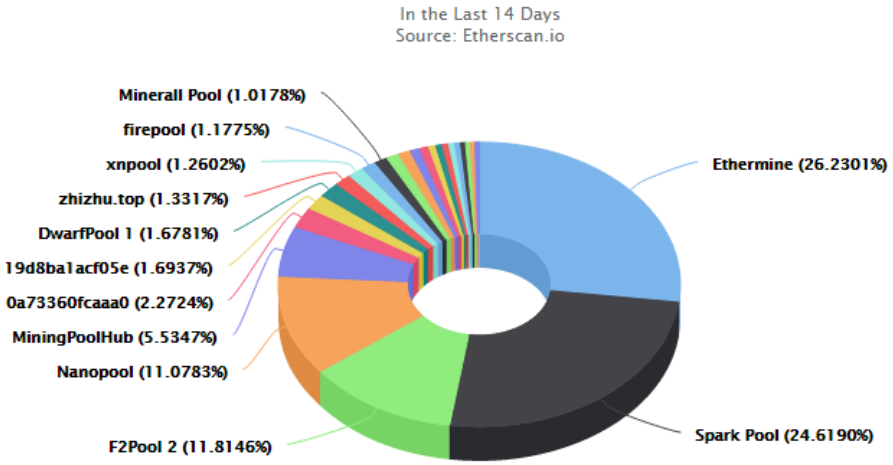
ETH 2.0 nie jest klasycznym forkiem, a zupełnie nową, niezależną siecią. Porzucenie aktualnego systemu i migracja na jego bardziej udoskonaloną wersję wiąże się przede wszystkim z małą wydajnością i brakiem możliwości skalowania on-chain w ETH 1.0 (ETH 1.0 to potocznie wykorzystywana nazwa aktualnego systemu, w opozycji do planowanych zmian i upgradeów, które zebrane zostały pod nazwą ETH 2.0). POW zapewnia nadzwyczajny poziom bezpieczeństwa sieci, a także jest świetnym fundamentem pod decentralizację. Decentralizacja nie jest w tym przypadku zaledwie pustym hasłem marketingowym, lecz cechą sieci, zapewniającą odporność na błędy, ataki i próby cenzury ze strony scentralizowanych jednostek decyzyjnych, jak np. organy rządowe. Niemniej, testy wykazały[5], że sieć ETH pod przewodnictwem protokołu POW jest w stanie przetworzyć zaledwie 20 transakcji na sekundę. (**Co prawda sama zmiana na POS nie umożliwia zwiększenia ilości transakcji – dzieje się to za sprawą shardingu.)** Jest to wartość wystarczająca dla globalnego, bezpiecznego systemu rozliczeniowego, gdyż zapewnia pełną stabilność sieci. Kiedy zaś pragniemy zbudować rozproszony superkomputer, z milionami inteligentnych umów (smart kontraktów), nowym rodzajem aplikacji (dApp), obsługujący pionierski typ cyfrowej ekonomii (DeFi), potrzebujemy czegoś więcej.

Jeszcze jednym kłopotem, który chcą rozwiązać architekci ETH jest koncentracja mocy obliczeniowej w rękach zaledwie kilku kopalni. Według Vitalika, POS i niski poziom wejścia w wysokości 32 ETH wymaganych do posiadania węzła walidującego transakcje, ma szansę zwiększyć decentralizację sieci.

[5] Ethereum 2.0 – A complete guide: https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-d46d8ac914ce



Rysunek 1: Statystki górnicze w sieci BTC



Rysunek 2: Statystki górnicze w sieci ETH.

W praktyce jednak sytuacja z POW i POS jest o wiele bardziej skomplikowana. Zastosowanie w kryptowalucie Dowodu Pracy (POW) ma mnóstwo pozytywnych aspektów – wysokie stężenie fizycznej mocy obliczeniowej wykorzystane do tworzenia bloków w sieci sprawia, że koszty ewentualnego ataku są niezwykle wysokie. Monopol na kontrolę sieci może również powstać w systemie korzystającym z POS, kiedy to zaledwie garstka graczy posiada przeważającą część zasobu kryptowaluty. Niemniej, ETH 2.0 zdaje się rozwiązywać część problemów, z którymi borykały się dotąd kryptowaluty oparte o POS.

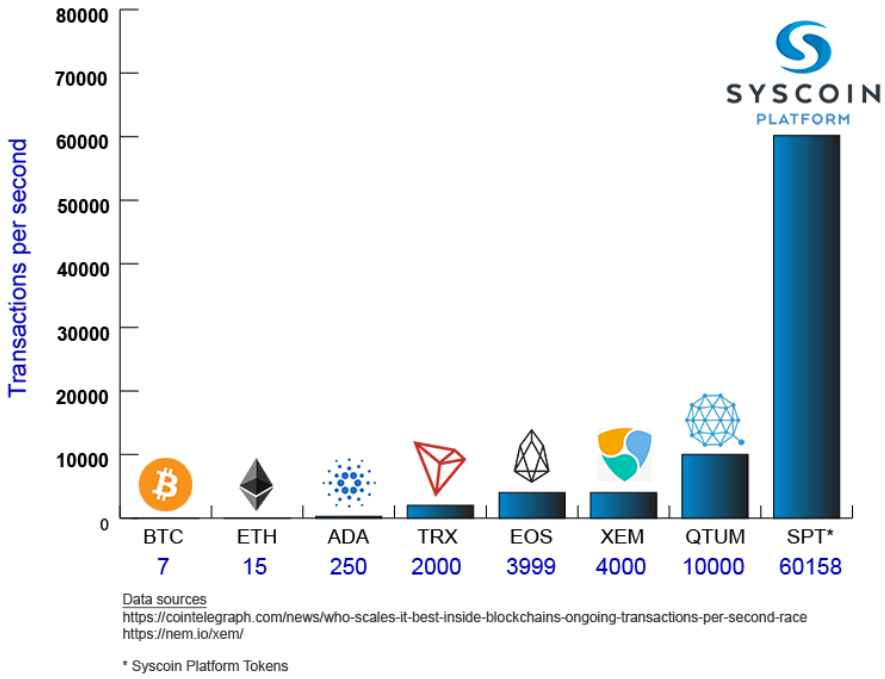
Problem skalowalności kryptowalut

Skalowalność jest chyba najczęściej podejmowanym tematem w społeczności kryptowalut. Różne metody – zwiększenie bloku, transakcje off-chain - proponowane są jako rozwiązania, mające w efekcie zwiększyć ilość transakcji na sekundę, jednocześnie nie zmniejszając decentralizacji (która w dużej mierze odpowiada za ogólne bezpieczeństwo sieci i niską podatność na ataki). Rozproszony charakter węzłów walidujących główny łańcuch sprawia, że nawet skoordynowany atak na sieć jest trudny do przeprowadzenia. Jeżeli takowy atak miałby szansę się powieść, POW i wykorzystana w nim energia sprawiają, że cofnięcie łańcucha lub podwójne wydatkowanie monet jest nieprawdopodobnie kosztowne. W przypadku Ethereum, godzina ataku na sieć kosztuje 130 tys. USD[6], przy czym potrzebowalibyśmy własnej infrastruktury sprzętowej, gdyż zaledwie 5% z wymaganych zasobów obliczeniowych może zostać wypożyczonych z usługi NiceHash.

Wiemy już, że o ile POW nadaje się do systemów takich jak Bitcoin – cyfrowych pieniędzy, w którym od ilości transakcji ważniejsza jest pewność, że transakcja zostanie przekazana, tak ETH próbuje osiągnąć inny cel. Nie jest walutą w tradycyjnej definicji tego pojęcia.

Projekty takie jak NEO, EOS, Stellar albo Ripple rzeczywiście oferują nieprawdopodobną liczbę TPS (transakcji na sekundę), a kolejne kryptowaluty promują się mówiąc o setkach tysięcy TPS.

[6] Pow attack costs. https://www.crypto51.app/



Rysunek 3: Przykład dążenia do jak najwyższej ilości transakcji na sekundę - Wyniki testu liczby TPS w kryptowalucie Syscoin.

Choć wyniki mogą, na pierwszy rzut oka, wyglądać imponująco, to jak dowodzę w archiwalnych raportach o NEO[7] i LISK[8], niemożliwe, na tą chwilę, jest skonstruowanie prawdziwie bezpiecznych i zdecentralizowanych kryptowalut osiągających przepustowość tysięcy transakcji na sekundę. Takie ilości TPS nie są do niczego potrzebne, jeżeli sieć nie jest wykorzystywana przez użytkowników. Wnioski płynące z dokumentu o Stellar (XLM)[9] pokazują, że w celu zwiększenia TPS zazwyczaj odrzuca się bezpieczeństwo, decentralizację i finalność transakcji. Takie zachowanie doprowadziło do poważnych konsekwencji – tydzień po opublikowaniu raportu, blockchain Stellar rzeczywiście uległ awarii i został wyłączony[10]. Jest to sytuacja, która nigdy nie powinna mieć miejsca w rozproszonych systemach. Na chwilę obecną, wydaje się, że drastyczne zwiększanie TPS (ponad poziom ok. 45 TPS) możliwe jest jedynie wtedy, gdy sieć jest scentralizowana. I nie jest to tylko hipoteza – dane przemawiają za siebie. EOS – 21 centralnie zarządzanych węzłów walidujących, NEO – mniej niż 10, wszystkie należące do Fundacji NEO lub pośrednio przez nią kontrolowane.

[7] NEO – Smart Economy
https://pl.scribd.com/document/407692118/NEO-RAPORT-by-stokarz
[8] LISK – Odkrywając potencjał technologii sidechain w zdecentralizowanych aplikacjach.
https://pl.scribd.com/document/411082413/Lisk-LSK-RAPORT-by-Stokarz
[9] Stellar – Konsensus raport.
https://pl.scribd.com/document/408530443/Stellar-Konsensus-RAPORT-by-stokarz
[10] Stellar blockchain goes offline: https://cointelegraph.com/news/stellars-blockchain-briefly-goes-offline-confirming-the-project-lacks-decentralization

Skalowanie kryptowalut jest trudne, gdyż każdy z węzłów w sieci musi zatwierdzić każdą z transakcji oraz dojść do porozumienia z innymi węzłami.

Ethereum na czele z Vitalikiem Buterinem zamierza podejść do problemu skalowalności w inny sposób.

Dlatego od 2014 roku prowadzone są liczne badania podstawowe oraz rozwijana jest teoria naukowa systemów rozproszonych i protokołów konsensusu pomiędzy węzłami w celu przyszłej optymalizacji łańcucha. W dalszej części raportu przyjrzymy się całemu spektrum nowości planowanych w Ethereum, będących wynikiem wytężonej pracy naukowej w latach 2014-2019. Każda z wymienionych technologii znajduje się na krawędzi poznanego – są to zazwyczaj pionierskie metody i systemy. Czytelnik musi zdawać sobie sprawę z egzotyki i eksperymentalnego charakteru proponowanych zmian. Choć setki genialnych umysłów wkładają całą swoją energię w to, aby wszystko działało jak należy, nie wiemy, jak długofalowo wpłynie to na sieć Ethereum. Mogą pojawić się nieplanowane błędy, bugi i krytyczne niedoskonałości w kodzie. Wszystko to może powodować znaczne ruchy w wycenie giełdowej Ethereum, gdyż każda z tych zmian wprowadza wysoką niepewność. Jeśli jednak ich wprowadzenie zakończy się sukcesem, Ethereum ma szansę wejść w zupełnie nową fazę i rzeczywiście stać się rozproszonym superkomputerem.

Czas w jakim zmiany pod nazwą ETH 2.0 – lub inaczej update Serenity, mają zostać wprowadzone, szacuje się na co najmniej kilka lat. W optymistycznym spojrzeniu, ETH 2.0 będzie gotowe w 2022 roku.

Uruchomienie Beacon Chain planowane jest już na 2019, w 2020 pewnie pojawią się pierwsze smart kontrakty WASM i możliwość migracji na nowy łańcuch, ostatecznie do 2022 powinien pojawić się sharding. - Tomasz Drwięga, Parity.

Zatem nie nastąpi to z dnia na dzień, a raczej będzie długotrwałym i żmudnym procesem, pełnym testów, sprzecznych doniesień medialnych o funkcjonowaniu nowej sieci, a także ogólnej niepewności. Dlatego pamiętajcie o wnioskach płynących z tego raportu, gdyż **fundamentalne zrozumienie nadchodzących technologii w ETH i odseparowanie szumu informacyjnego, będzie odgrywało kluczową rolę w przyszłych decyzjach inwestycyjnych.**

Zmiany w Ethereum

ETH 2.0, nazywane Serenity[11], zawierać będzie technologie takie jak: Casper[12] FFG, Sharding, Beacon Chain i eWASM. Dodatkowo, powstają liczne rozwiązania kategorii 2nd Layer (z ang. „druga warstwa" – zazwyczaj są to technologie off-chain, w których większość aktywności dzieje się poza łańcuchem głównym, odciążając go, a następnie, gdy już wszystkie interakcje między użytkownikami są skończone (gdy dochodzi do konfliktu między uczestnikami to przechodzi się na główny łańcuch, który pełni rolę arbitra), finalna wersja transmitowana jest na główny łańcuch). Są to ZK-STARKs, Zether, Plasma i State Channels (kanały off-chain, podobne do Lightning Network). Wszystko to ma sprawić, że Ethereum będzie szybkie, tanie w użyciu oraz prywatne.

Dla pełnego zrozumienia musimy cofnąć się i zobaczyć, jaka ogólnie myśl przyświeca deweloperom ETH od samego początku. Każda z tych technologii zostanie szczegółowo omówiona w dalszej części raportu.

Odkąd w 2014 roku Ethereum zostało finalnie przedstawione społeczności kryptowalut, przechodzi nieustanne zmiany, mające na celu udoskonalenie kryptowaluty i osiągnięcie jej finalnego celu. Stania się globalnym komputerem. Jak na razie cel ten nie został osiągnięty, jednak ogólny obraz rozwoju Ethereum, jaki możemy prześledzić na przestrzeni ostatnich lat, jest nadzwyczaj pozytywny i napawa optymizmem. Deweloperzy ETH, zamiast spieszyć się z niesprawdzonymi i niestabilnymi implementacjami pionierskich technologii, które rozwijane są od końca 2014r., stosują długofalowe podejście – małe zmiany, prowadzące do jasno określonego, większego celu.

[11] Serenity. What will it bring? : Serenity, What will it bring? : https://blog.goodaudience.com/waiting-for-serenity-what-will-it-bring-3144f4f19c1c

[12] Partially explained Casper specs: https://medium.com/@barnabe/partially-explained-casper-cbc-specs-86d055fd0628

Rysunek 4: Historia aktualizacji głównego protokołu ETH

Niedawno uznano, że sieć Ethereum jest gotowa, aby wejść w kolejną fazę. Plan na następne kilka lat wszedł do gry.

Od ponad roku Ethereum rozpoczęło wdrażanie dużych zmian, fundamentalnie reorganizujących sposób, w jaki funkcjonuje sieć. Pomimo tego, że za przywódców głównej myśli technicznej Ethereum uznać można Vitalika Buterina, Justina Drake'a i Vlada Zamfira – trzy z osób posiadające spory wpływ na rozwój kryptowaluty (choć Vlad zdystansował się trochę od projektu od czasów ETH 1.0) – to nawet oni, proponując jakiekolwiek zmiany, muszą uzyskać akceptację na drodze ogólnego konsensusu wszystkich użytkowników sieci. Proces implementacji zmian w Ethereum jest taki sam jak w przypadku większości kryptowalut. Mamy do czynienia z systemem EIP – Propozycja Zmian w Ethereum (Ethereum Improvement Proposal).

Udoskonalenia te, w szczególności tegoroczny hardfork Konstantynopol, były wprowadzeniem do ETH 2.0. Ograniczono nagrodę dla górników z bloków, opóźniono bombę trudności, aby dać więcej czasu na wprowadzenie zmian – mechanizm mający sprawić, że kopanie ETH stanie się nieopłacalne (bomba ma długofalowo wręcz zmusić społeczność do wprowadzania zmian i udoskonaleń), a także dodano liczne poprawki, takie jak zmniejszone koszty „State Channels", które są jednym z głównych, przyszłych rozwiązań skalowalności off-chain dla ETH.

Rysunek 5: Przedstawienie udoskonaleń w ramach hardforka Constantinopol

ETH 2.0 jest potężnym projektem z długofalową wizją. Dlaczego?

- Fundamentalne prace nad teorią, a później kodem, trwały nieprzerwanie od 2014 roku (kiedy to po raz pierwszy pojawił się pomysł migracji na POS – Vitalik zaprezentował wtedy koncept Slashera[13] - ETH z Proof of Stake).
- Testowanie i pełne wdrożenie ETH 2.0 trwać będzie przez najbliższe kilka lat.
- Aby osiągnąć zakładane cele, deweloperzy musieli zmierzyć się z wcześniej nierozwiązanymi problemami zdecentralizowanych systemów opartych o protokół POS, jak na przykład: problem „nothing at stake[14]".

[13] History of Casper. Part I – Slasher: https://medium.com/@Vlad_Zamfir/the-history-of-casper-part-1-59233819c9a9
[14] Understanding Proof of Stake: The nothing at stake Theorem: https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

The Ethereum Roadmap at a Glance

Upgrade	Date	Details
Raiden Red Eyes	December 2018	Off-chain solution for faster and cheaper transactions.
Constantinople hard fork	January 16th, 2019	Lays the technical groundwork for significant scaling projects in the future.
Plasma	TBD	The introduction of "child" chains off the main Ethereum blockchain for faster and cheaper transactions. Similar to how the Lightning Network works on Bitcoin.
Casper	mid-2019	Ethereum's main scaling goal. Casper is the shift from Proof-of-Work to the more efficient Proof-of-Stake.
Sharding	2020-2021	Partition the existing blockchain into smaller pieces known as shards.
Serenity (aka Ethereum 2.0)	2019-2021	The culmination of Casper and Sharding will create "Ethereum 2.0."
Ethereum 3.0	2022-2025	Implementation of a 'super quadratic sharding' solution which could facilitate one billion transactions per day.

Rysunek 6: Roadmap Ethereum

Ethereum 2.0 – inaczej określane jako update Serenity, filozofię swojej bazowej architektury zawiera w kilku głównych punktach:

- Decentralizacja – aby umożliwić każdej osobie posiadającej średniej klasy laptopa zdeponowanie ETH i walidację transakcji/shardów.
- Długowieczność – aby sieć była w stanie pozostać aktywna nawet w przypadku kiedy przeważająca większość węzłów walidujących zostałaby wyłączona (np. gdyby było to działanie celowe, międzynarodowa cenzura, lub wielkoskalowy kataklizm naturalny).
- Bezpieczeństwo i Odporność – oprócz decentralizacji, która drastycznie zwiększa koszty potencjalnego ataku, przygotować ETH na możliwe zagrożenia płynące z przyszłych komputerów kwantowych, aka. wprowadzić narzędzie do szybkiej implementacji protokołów kryptograficznych, o których zakłada się, że są odporne na np. algorytm Shora[15]. (choć nie jest to priorytetem)
- Prostota – zmniejszenie skomplikowania systemu, nawet za cenę wydajności.

Ethereum ma być zatem rozproszone (jak na prawdziwy globalny komputer przystało), łańcuch ma mieć zdolność pozostania live nawet jeśli większość węzłów zostanie nagle odłączona, mają powstać mechanizmy szybkiego reagowania na zmieniające się zagrożenia od strony

[15] Algorytm faktoryzacji Shora. Jak kwantowe komputery mogą łamać standardowe szyfrowanie: https://www.youtube.com/watch?v=lvTqbM5Dq4Q

technologii komputerów kwantowych, które zakłada się, że będą zdolne łamać klasyczne szyfrowanie, w tym kryptografię krzywych eliptycznych stosowaną w Ethereum. Kryptowaluta ma również być przyjazna dla deweloperów, prosta i łatwa w użyciu. System smart kontraktów musi być intuicyjny oraz przystępny, aby zwiększyła się adopcja.

Ethereum i szlak ku decentralizacji – realne wnioski

Załóżmy na chwilę, że mamy rok 2022/2023. Każde z udoskonaleń kryptowaluty zostało zaimplementowane z sukcesem. Jak w takim razie wygląda Ethereum 2.0?

- Liczne aplikacje Plasmy i state channels, jako rozwiązania off-chain, pozwalają na szybkie i bezpieczne mikropłatności i mikrotransakcje, nieobciążając tym samym łańcucha głównego.
- Skalowalność on-chain wzrosła prawie 1000x, dzięki dzieleniu węzłów na „shardy".
- Deponowanie smart kontraktów na nowej maszynie wirtualnej eWASM jest tanie i szybkie.
- Ethereum działa w pełni korzystając z algorytm konsensusu Proof of Stake - Casper.
- Technologia STARKS i Zether uczyniły Ethereum nie tylko anonimowym, lecz również nadały mu cech prywatnościowych, zwiększając tym samym bezpieczeństwo użycia kryptowaluty.

Choć daleko mi od optymizmu wyrażanego przez jednego z współzałożycieli Ethereum i szefa firmy Consensys – Josepha Lubina, mówiącego o tym, że w ciągu dwóch lat możliwości Ethereum wzrosną ponad tysiąckrotnie[16], po niezwykle szczegółowej, ponad dwutygodniowej analizie każdego, nawet najdrobniejszego aspektu technologii, które zostaną wprowadzone w ETH 2.0 i ETH 3.0, **uważam, że w przeciągu 5 następnych lat, projekt Ethereum stanie się podstawowym komponentem nowej branży systemów rozproszonych. Ethereum będzie szybkie, bezpieczne, tanie i prywatne.** Nie będąc walutą jak Bitcoin czy Monero, ma szansę uniknąć bycia zdelegalizowanym przez rządy państw, w obawie o utratę władzy nad systemem monetarnym.

[16] Joseph Lubin. Ethereum will expand 1,000. Invest in Blockchain.
https://www.investinblockchain.com/joseph-lubin-ethereum-will-expand-1000x-in-just-2-years/

ETH 2.0 – Serenity

Serenity wprowadzi do Ethereum system POS – Proof of Stake. Eliminuje on górników, a rolę walidatorów transakcji przejmują osoby posiadające określoną ilość jednostki danej kryptowaluty. W tym wypadku jest to Ether. Jeśli pragniesz być jednym ze „stróżów" sieci – za co otrzymujesz niewielką nagrodę – musisz zdeponować wymagane kryptowaluty w specjalnym smart kontrakcie.

Rysunek 7: Analogią POS może być umieszczenie depozytu na lokacie bankowej – tylko, że musimy pozostać aktywni

Bardzo początkowe plany deweloperów Ethereum zakładały, że wymaganym depozytem będzie 1500 ETH, czyli 427 tys. USD po aktualnej cenie rynkowej. Miało to jednak miejsce wiele lat temu i nie spodziewano się jednak tak ogromnego wzrostu ceny Ethereum. Nowy pomysł, posiłkujący się teorią gier, zakłada wymóg zdeponowania 32 ETH, aby móc potwierdzać transakcje. Niecałe 10 tys. USD brzmi już zdecydowanie lepiej

Rysunek 8: Porównanie starego i nowego planu deweloperskiego

Faza 0[17]

Mająca wejść w życie tego lata[18], faza zero, rozpoczyna proces migracji ETH na POS[19]. Stworzony zostanie zupełnie nowy łańcuch nazywany Beacon Chain. Będzie on niezależny od zwykłego ETH. Pierwsi deweloperzy i entuzjaści będą w stanie zamienić swoją kryptowalutę Ethereum na jej odpowiednik w Beacon Chain i już teraz rozpocząć stakowanie w POS. Niemniej, nie zalecam tego robić, gdyż aż do Fazy 2, która rozpocząć może się nawet za dwa lata, nie będziemy **prawdopodobnie** mieli dostępu do posiadanych przez nas ETH. Owszem, otrzymamy nagrody ze stakowania, jednak niemożliwe będzie upłynnienie posiadanego ETH, gdyż będzie ono zablokowane w smart kontrakcie w sieci Beacon. Bilet w jedną stronę. ETH z oryginalnego łańcucha ulegnie znieszczeniu.

ETH 1.0 wykorzysta Casper FFG[20] – Friendly Finality Gadget. FFG nie jest pełną wersją POS, a raczej skomplikowaną technicznie hybrydą pomiędzy POS, a POW. Opracowana przez Vitalika Buterina, w fazie zero posłuży jako technologia zapewniająca finalność w przesyłanych transakcjach (finalność sprawia, że transakcja nie może być teoretycznie cofnięta w czasie potencjalnego ataku).

Important Considerations

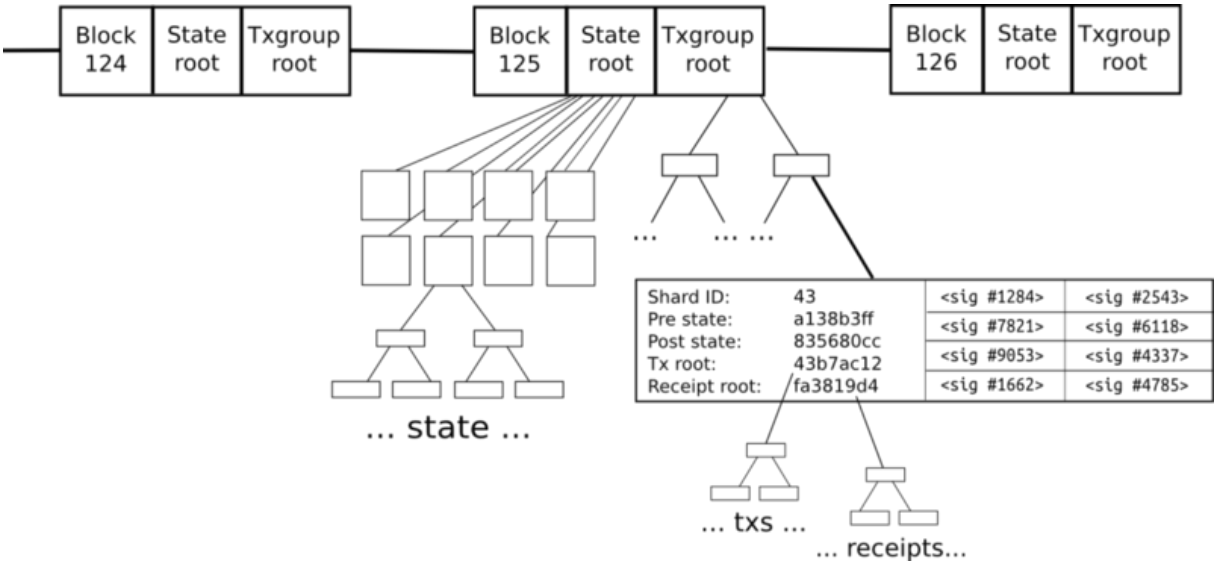
- ETH2 is transferable to and from shards once Phase 2 is complete.
- There will be a minimum amount of ETH stake needed in order to first bootstrap the beacon chain. This is defined as `CHAIN_START_FULL_DEPOSIT_THRESHOLD` in the deposit contract that will live on the Eth 1.0 chain. Currently, this is set to 16384 validators needed. That would mean 524,288 ETH in total stake is needed. This would pay ~11% interest to stakers.
- To become a validator, you'll need to stake 32 ETH2.
- During Phase 0, all user transactions and smart contract computations will still occur on the Eth 1.0 chain.

Rysunek 9: Źródło - Ethereum Developer Portal

[17] Ethereum Roadmap Phases: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/
[18] The Future of Ethereum: A Scaling Roadmap to Casper, Plasma and Sharding: https://blockexplorer.com/news/ethereum-scaling-roadmap-casper-plasma-sharding/
[19] Ethereum POS: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[20] Casper FFG Whitepaper: https://arxiv.org/pdf/1710.09437.pdf

Faza 1[21]

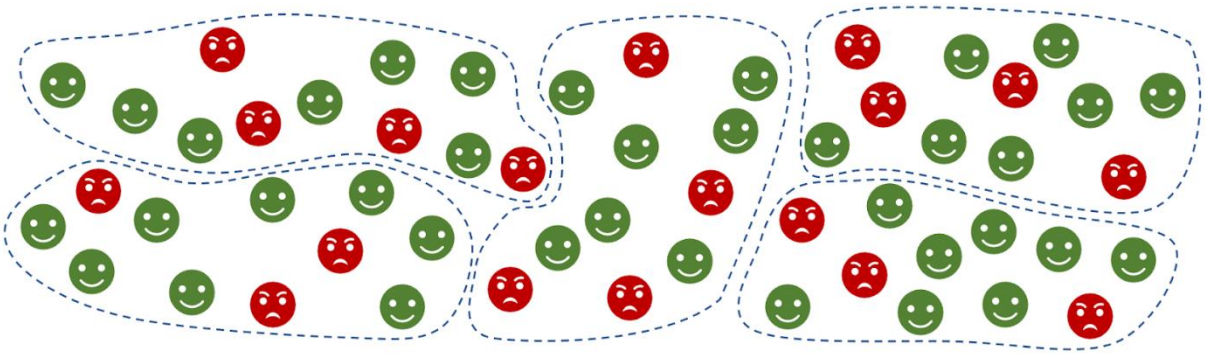
W tej fazie nie czeka nas wiele nowości. Planowane są pierwsze, wstępne implementacje technologii shardingu - czyli dzielenia wszystkich danych i transakcji na blockchainie na mniejsze części które mogą działać niezależnie od siebie i w tym samym czasie.



Rysunek 10: Model shardingu w blockchainie

Sharding docelowo ma zmienić sposób w jaki węzły odbierają i przesyłają między sobą informacje o transakcjach i smart kontraktach. Teoretyzuje się, że dzięki temu, nawet w przypadku kiedy znaczna część węzłów walidujących stanie się „złośliwa", będąc realnym zagrożeniem dla stabilności i dalszego funkcjonowaniu danego blockchaina, shardy pozwolą na tak specyficzne pogrupowanie nodów, że mimo złośliwych uczestników, możliwe będzie dojście do globalnego konsensus. Problemem shardingu jest to, że jeśli podzielimy blockchain na części – shardy i następnie przydzielimy wszystkich „złośliwych" użytkowników do jednego sharda, mogą oni skutecznie zaatakować sieć. Aby tego uniknąć, zakłada się wprowadzenie mechanizmu, który przydzielanie walidatorów do shardów czyniłby w sposób całkowicie losowy i zarazem deterministyczny oraz transparentny. Lecz jest to niezwykle trudne zadanie, zatem obecny plan deweloperów jest taki, aby zbudować tzw. Randomness Beacon oparty o Verifiable Delay Functions (VDFs).

[21] Mango Research: Ethereum Roadmap Update: https://www.mangoresearch.co/ethereum-roadmap-update/



Rysunek 11: Model konsensusu, gdy węzły podzielone są na grupy. Podobne rozwiązanie stosuje Stellar (XLM)

W Fazie 1, główny łańcuch Ethereum ciągle będzie funkcjonował. Nagrody wypłacane będą zarówno górnikom jak i osobom stakującym BETH (ETH przeniesione na Beacon Chain) w Beacon Chain. Początkowo dojdzie zatem do drastycznego skoku inflacji. Jest to poważne zagrożenie, szczególnie dla inwestorów (choć nie będą to płynne aktywa, może spowodować małą panikę). Jeżeli nie pojawi się nowy popyt na Ethereum, to chwilowa wysoka inflacja może zbić cenę Ethereum. Mimo tego, modele zakładają, że inflacja zacznie zmniejszać się do poziomu 0-1%, wraz z powolnym wygaszaniem górnictwa i POW oraz migracją na POS. Jeśli miałbym dokonywać predykcji związanych z tym tematem, powiedziałbym, że rosnąca euforia związana z nową technologią, skutecznie wymaże z ludzkiej świadomości pojęcie o wysokiej inflacji i popyt przewyższy rosnącą podaż. Choć mogę się całkowicie mylić.

Important Considerations

- In Phase 0, 1, and 2 the main PoW chain (Eth 1.0) will remain live while testing and transitioning is happening on the Eth 2.0 chain. This means that rewards will be paid to both Ethereum 2.0 validators as well as the normal PoW block rewards. Therefore, the combined inflation of the 2 chains may spike initially but then start to trend towards the 0-1% range as the PoW chain is gradually deemphasized.

Rysunek 12: Cele Fazy 1

Faza 2

Wstępnie planowana na 2021 rok faza druga to czas, w którym Ethereum zacznie wreszcie (miejmy nadzieję) błyszczeć. Czego możemy się spodziewać?

- Przejścia na pełny POS – Casper CBC[22].
- Sharding na głównym łańcuchu.
- Zmiany aktualnej wirtualnej maszyny Ethereum na nową, lepszą wersję eWASM.

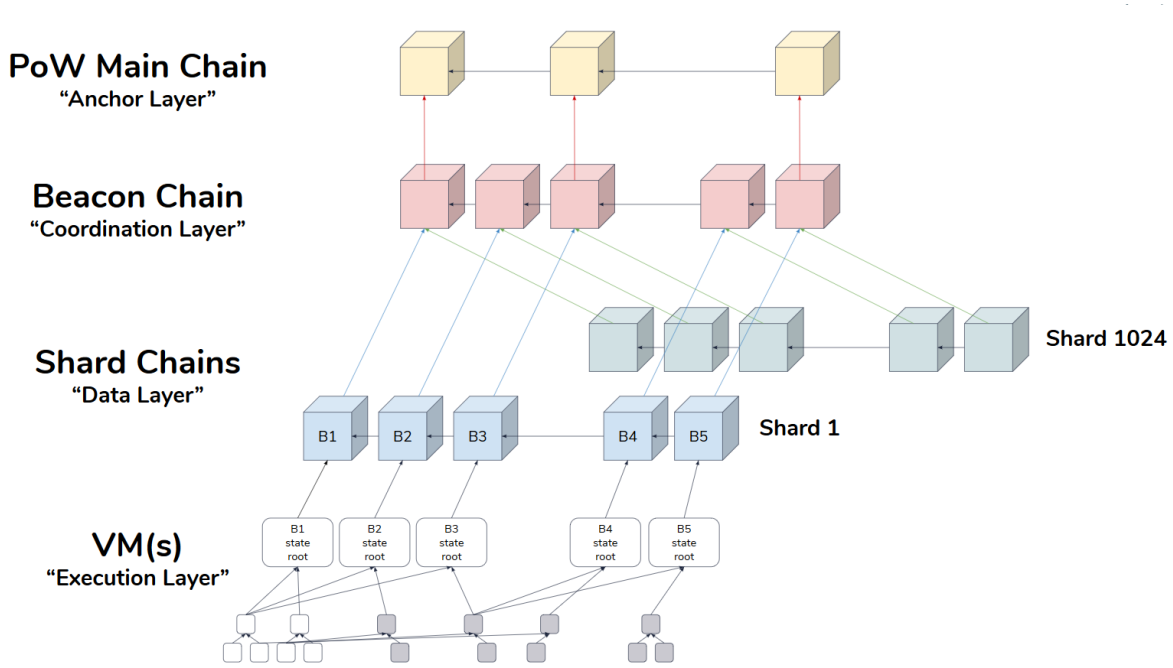
Jeżeli plan się powiedzie, to za dwa lata, górników Ethereum obejrzeć będziemy mogli co najwyżej w muzeum. Faza druga oznacza kilkunastokrotnie szybsze Ethereum[23], z wydajnymi i przystępnymi w cenie smart kontraktami. Jeżeli Ethereum uda się sprawić, że inteligentne umowy w końcu będą tanie, zdeklasuje tym większość swoich konkurentów*.

Wraz z pełnym POS, rozwiązany zostanie jeszcze jeden problem dręczący kryptowaluty tego typu. Co zrobić w momencie, gdy część z węzłów wejdzie w tryb offline. Dotychczas, niemożliwym do wykrycia było czy zaszło to specjalnie, czy to większa grupa węzłów cenzuruje informacje napływające z mniejszości, przez co stara się pozyskać większą porcję nagrody ze stakowania dla siebie. Casper CBC wprowadza zatem system kar, dzięki któremu takie zachowanie staje się ekonomicznie nieopłacalne. Casper zmusza więc węzły do zachowywania się uczciwie w stosunku do sieci i jej uczestników. W przeciwnym razie, sieć zabiera im część depozytów Etheru złożonego w smart kontraktach.

Nie sposób zaprzeczyć, że architektura nowego Ethereum, mimo zapewnień o dążeniu do prostoty, wydaje się być niesamowicie skomplikowana. I owszem, w początkowej fazie przemian protokołu, tak właśnie będzie. Poniższy obraz przedstawia graficzną wizualizację bloków i zależności między nimi w ETH 2.0.

[22] Casper CBC and formal verification:
https://medium.com/layerx/cbc-casper-and-formal-verification-1954cbd1d971
[23] A complete guide to Ethereum 2.0 :
https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-d46d8ac914ce

* Wycenę kosztów deponowania smart kontraktów w różnych projektach kryptowalutowych, znajdziesz w raporcie: „LISK – Odkrywając potencjał technologii Sidechain, w zdecentralizowanych aplikacjach”.



Rysunek 13: Schemat funkcjonowania bloków w Ethereum 2.0.

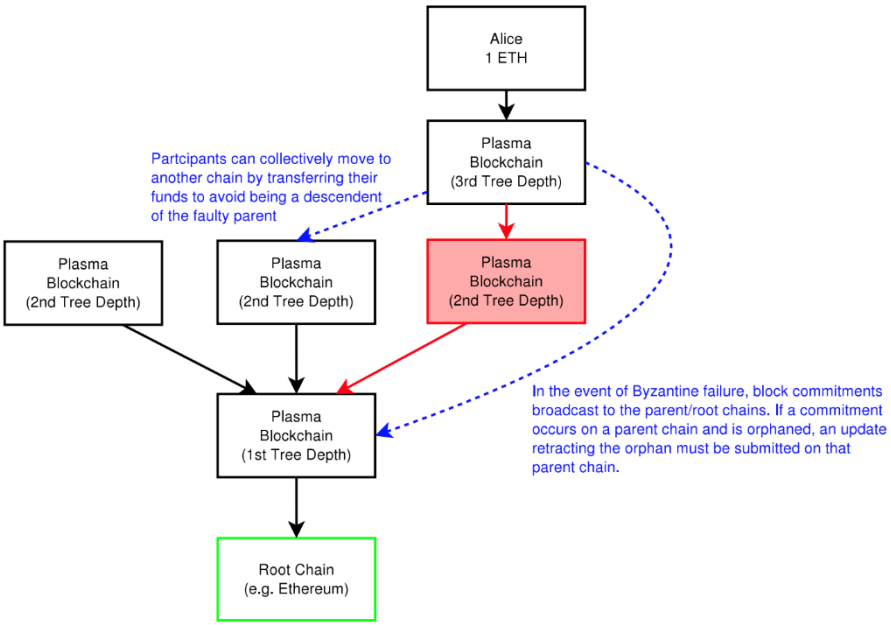
Druga Warstwa, rozwiązania off-chain

Optymistyczne spojrzenie na przyszłość Ethereum napędzane jest również, w dużej mierze, przez grupę technologii mającą przenieść ruch z głównego łańcucha, na mniej bezpieczne, ale za to szybsze kanały poza nim. Tak samo jak w przypadku Lightning Network znanego z Bitcoina, technologie off-chain nie wpływają, ani negatywnie, ani pozytywnie na główny łańcuch. Są od niego niezależne, neutralne. Jeżeli zawiodą, mainchain nie ucierpi na tym. Jeśli okażą się sukcesem, a użytkownicy zaufają technologii, przyjdzie płynność i adopcja, to staną się silnym narzędziem uzupełniającym projekt. Wymieńmy teraz kilka z nich:

- Plasma
- State Channels
- ZK-STARKS
- Zether

Plasma

Sidechainy zbudowane według architektury podobnej do Merkle Tree (Drzewo Hash, Drzewo Skrótów). Wykorzystując Plasmę, dowolny użytkownik mógłby otworzyć swój „kanał”, stworzyć swój łańcuch boczny, dzięki któremu przeniósłby część ruchu normalnie wykonywanego na łańcuchu głównym, poza sieć.



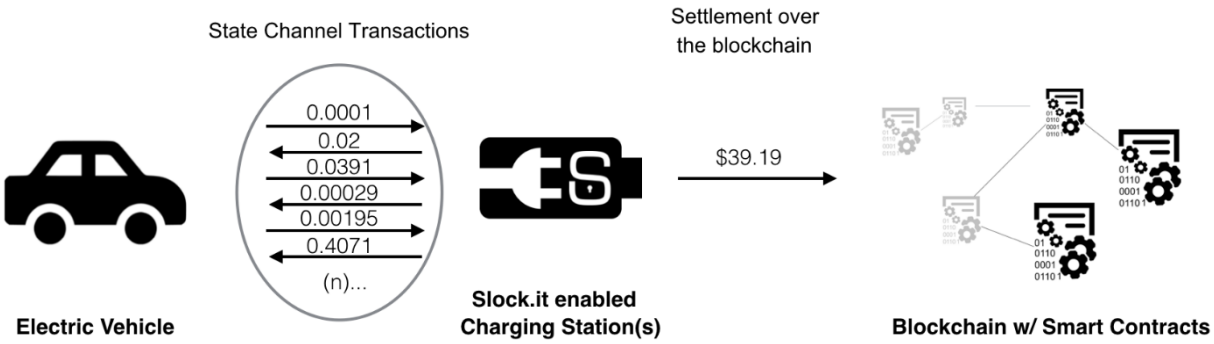
Rysunek 14: Wizualizacja funkcjonowania Plasmy

Rodzaje interakcji mogące zachodzić w obrębie łańcuchów bocznych albo między nimi to, między innymi: mikrotransakcje, smart kontrakty lub lokalne aplikacje (wykorzystywane jedynie przez grupę użytkowników, którzy następnie transmitowaliby finalny obraz sieci bocznej na łańcuch główny – można by sobie wyobrazić szkolny projekt budowany na jednym z kanałów Plasmy, a następnie, np. z końcem każdego dnia, dane przesyłane byłyby na mainnet Ethereum, gdzie zostałyby zabezpieczone i dostępne, dla grupy użytkowników, z każdego miejsca na świecie). Ciężko jest oszacować zakres ludzkiej kreatywności w obliczu takiej technologii – być może moje predykcje są całkowicie nietrafione, a Plasma wykorzystywana będzie do zupełnie innych celów.

State Channel

Jest to w istocie dwukierunkowy kanał dyskusyjny[24] między użytkownikami lub użytkownikiem, a usługą (maszyną). Wiadomości przybierają formę transakcji, takich jak „Chcę kupić piwo za 3 $" lub „Chcę wynająć ten kanał telewizyjny na godzinę za 5 $". Uczestnicy podpisują każdą z informacji, uniemożliwiając późniejsze zanegowanie serii transakcji.

Transakcje te odbywają się całkowicie poza główną siecią bloków i wyłącznie pomiędzy uczestnikami. Co oznacza, że są tanie i bardzo szybkie do wykonania w porównaniu ze standardowymi płatnościami na blockchainie. Mogą jednak pojawić się problemy z bezpieczeństwem – jeśli wykryjemy jakąś nieprawidłowość, można odwołać się do głównego łańcucha, lecz aby to zrobić, musimy być, teoretycznie, cały czas on-line, kiedy kanał jest otwarty. W praktyce przewiduje się, że za drobną opłatą będzie można taki monitoring zlecić trzeciej stronie.



Rysunek 15: Model State Channel na Ethereum

Idea state channels jest prosta – wprowadzać do łańcucha głównego tylko te dane, które są całkowicie konieczne. Mimo że, jestem zdania, że ilości danych przesyłanych na blockchain musi ulec zmniejszeniu (ze względu na koszty – dlatego proste kryptowaluty, takie jak Bitcoin, służące tylko do jednego rodzaju aktywności: płatności, są moim zdaniem najlepszym zastosowaniem kryptografii i blockchaina), to sądzę, że rozwiązania typu State Channels, **są zbędną komplikacją i powinno się je zaliczać do zewnętrznych aplikacji, kompatybilnych z Ethereum.** W żadnym przecież scenariuszu, kanały te nie są zabezpieczane przez sieć główną – dopiero finalne wprowadzenie informacji na blockchain Ethereum sprawia, że mają one cokolwiek wspólnego z kryptowalutami.

[24] State Channels Ethereum: https://blog.stephantual.com/what-are-state-channels-32a81f7accab

ZK-STARKS[25] i Zether.

Udoskonalenie technologii znanej z kryptowaluty Zcash. Pozwala na zmniejszenie i optymalizację wielkości transakcji, jednocześnie czyniąc je w pełni prywatnymi. Dzięki temu konstruktowi kryptograficznemu, jako użytkownik, jesteśmy w stanie potwierdzić, że posiadamy określoną informację bez ujawniania jej adresatowi.

Wraz z Zether[26]- nowym rodzajem smart kontraktu, który sprawia, że balans naszego adresu nie jest widoczny, czyniąc tym samym transakcje prywatnymi, technologie te mają szansę wprowadzić cechę rzeczywistej prywatności do Ethereum. Jeżeli to się uda, na znaczeniu stracić mogą, dotąd znane jedynie ze swojej prywatności kryptowaluty jak Zcash i Monero (choć w raporcie pt.: „Zcash – rozwiązując zagadkę prywatności kryptowalut" udowadniam, że Zcash nie jest aktualnie prywatny przez zbyt wysokie wykorzystanie nieprywatnych adresów typu „T" i nie powinien być do tych celów wykorzystywany). Szczególnie jeśli Ethereum uda się skalować – czego nie można powiedzieć o Monero.

Podsumowanie Serenity

Uważam, że wysokim błędem byłoby nie docenić potencjału kryjącego się za Ethereum i grupą deweloperów, która pracuje nad ekosystemem. Coś co dziś wydaje nam się prawie niemożliwe – jak chociażby skuteczne skalowanie on-chain, być może w rzeczywistości nie jest trudne do rozwiązania. Czy Ethereum to się uda? Nie wiem, zamierzam jednak postawić na prawdopodobieństwo sukcesu. Dokładana analiza Serenity pokazała, że nie jest to tylko wprowadzenie nowego śmiesznego i nieużyteczne wynalazku. Mamy do czynienia z nauką w pięknej jej postaci oraz, miejmy nadzieję, skuteczną implementacją teorii w praktyce. Jeżeli to się nie uda, cóż – Ethereum pamiętać będziemy jako największy i najdroższy technologiczny plac zabaw na świecie.

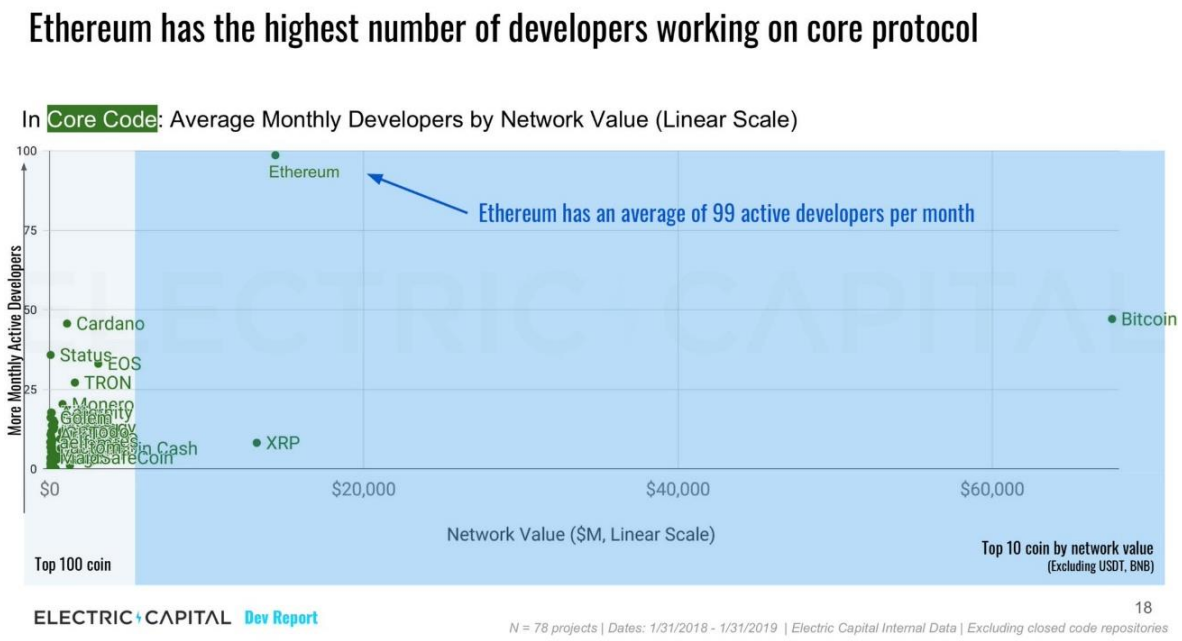
Są wysokie szanse, że na przestrzeni od 3 do 5 lat, Ethereum będzie posiadało funkcje prywatności, można będzie skalować aktywność użytkowników on-chain, a smart kontrakty staną się przystępne do wykorzystania. W następnym rozdziale przyjrzymy się aktywności sieci oraz określimy, jakie zagrożenia mogą przeszkodzić Ethereum w realizacji planów. Dowiemy

[25] ZK STARKS for Ethereum blockchain:
https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-starks/
[26] Zether: Towards Privacy in a Smart Contract World:
https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-starks/

się również, kto depcze Ethereum po piętach, chcąc jako pierwszy uzyskać miano globalnego komputera.

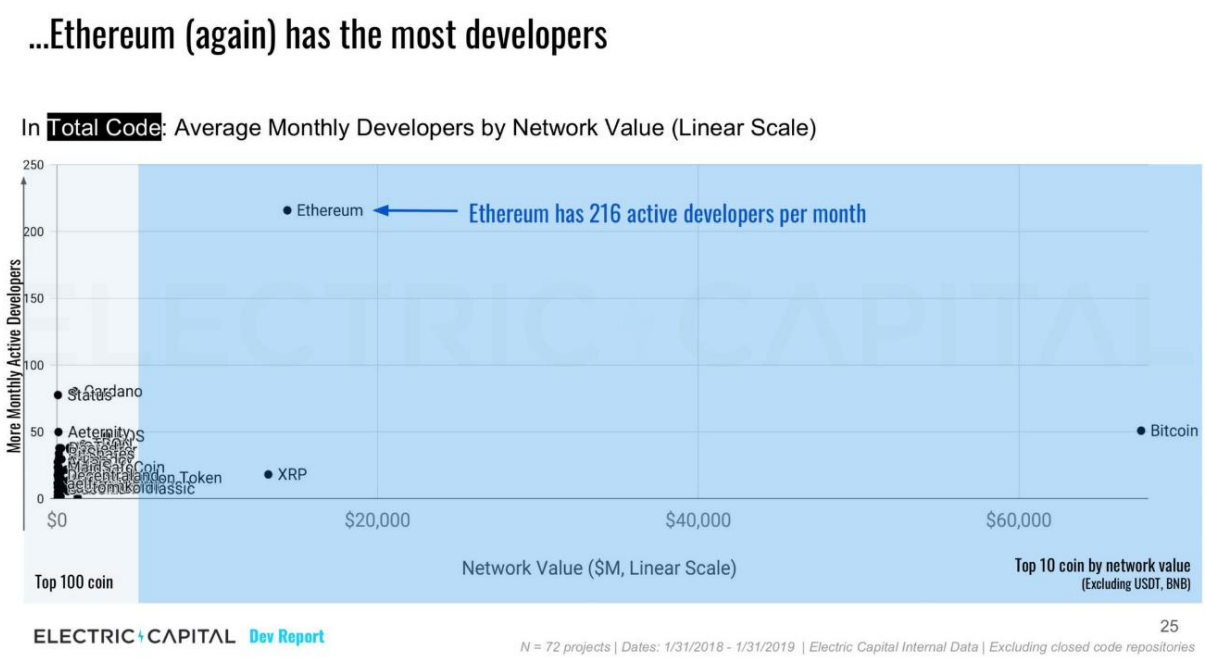
Ethereum – Statystki

Ethereum posiada najwięcej aktywnych deweloperów w ujęciu miesięcznym.



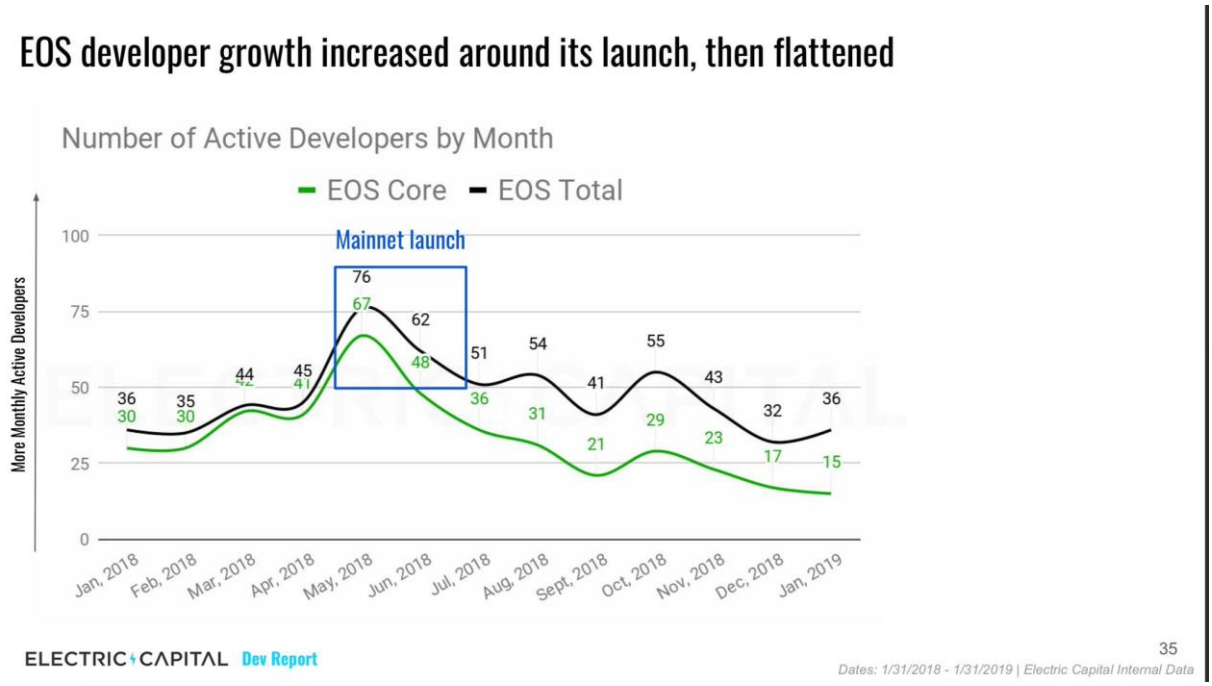
Rysunek 16: Deweloperzy pracujący nad ETH Core.

Łącznie średnio 216 osób pracuje nad wszystkimi inicjatywami związanymi z Ethereum (pamiętajcie, jest to publiczna lista osób wprowadzająca zmiany na Githubie – statystyka ta nie liczy również deweloperów z projektów takich jak np.: Parity Technologies, Loom Network czy OmiseGo, którzy również budują technologię dla Ethereum).



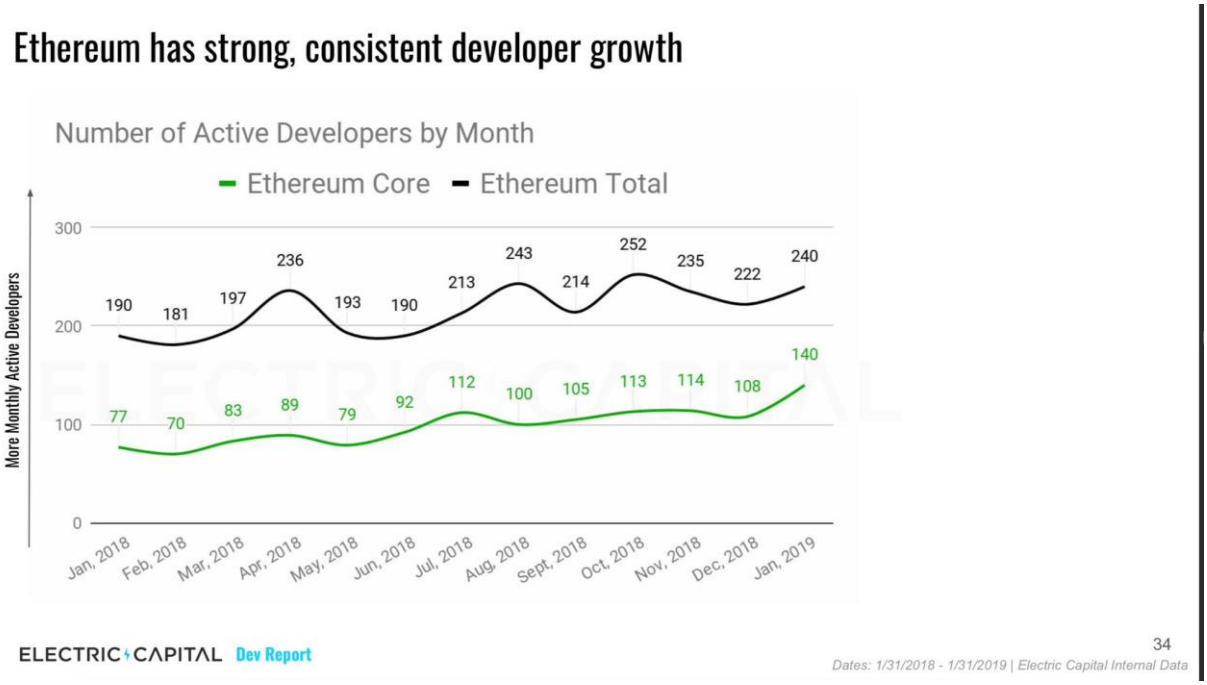
Rysunek 17: Ilość deweloperów aktywnie pracująca nad Ethereum.

Dla porównania, jeden z czołowych konkurentów ETH – EOS, posiada średnio 36 deweloperów pracujących nad projektem, z czego raptem 15-20 rozwija główny protokół EOS Core.



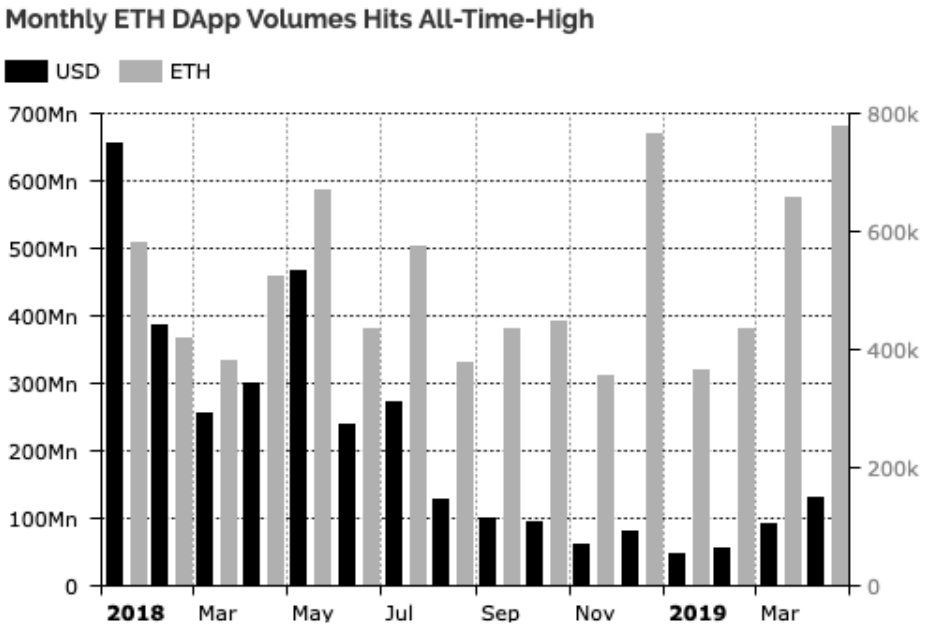
Rysunek 18: Deweloperzy EOS

Z miesiąca na miesiąc Ethereum zdaje się przyciągać coraz więcej inżynierów oprogramowania, co potwierdza ta statystyka:



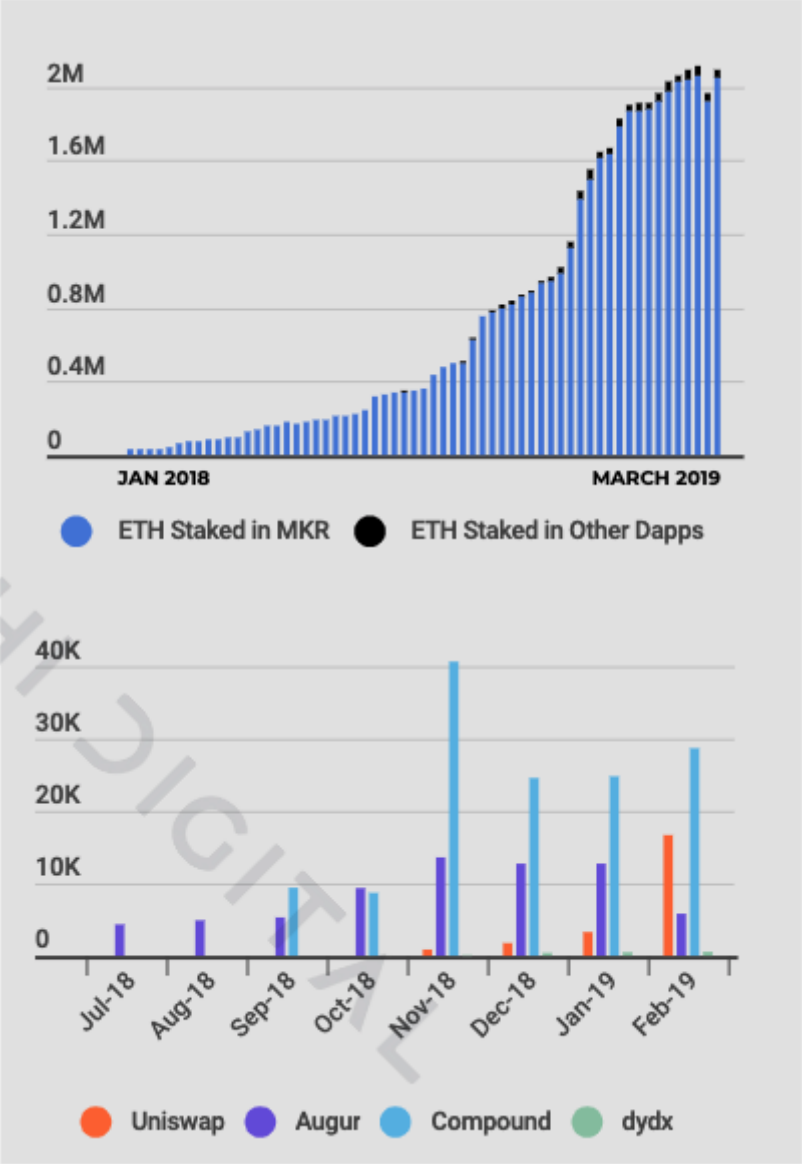
Rysunek 19: Wzrost liczby deweloperów na przestrzeni roku. Dane pochodzą ze stycznia 2019 roku.

W marcu tego roku, wolumen Etheru przepływającego przez zdecentralizowane aplikacje osiągnął najwyższą wartość w historii (dane mierzone w ETH, nie USD!):



Rysunek 20: Rozkład miesięcznego wolumenu ETH w dApp'ach.

Największym jednak zainteresowaniem zdają się cieszy technologie z nowej dziedziny zdecentralizowanych finansów – DeFi. Łączny wolumen ETH przepływający przez projekty DeFi prezentuje się następująco:

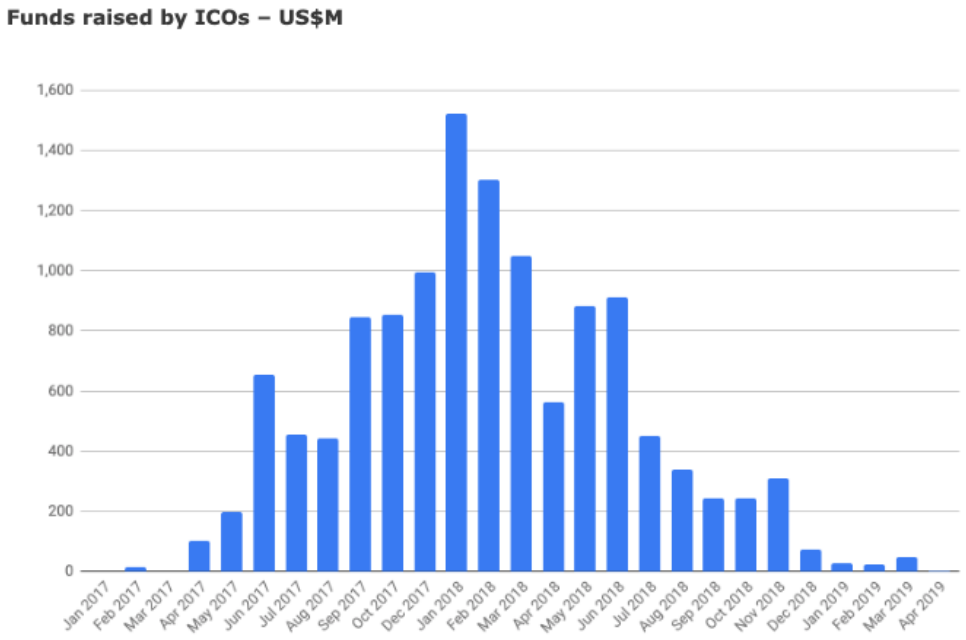


Rysunek 21: ETH w dApp - źródło: Delphi Digital

Sentyment rynku jest bardzo pozytywny:

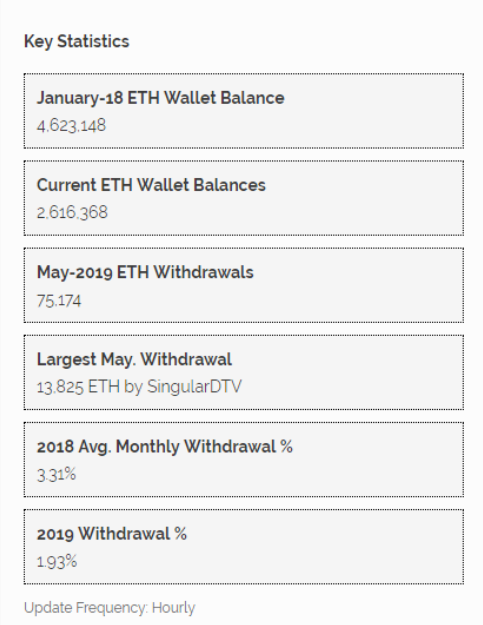
Rysunek 22: Sentyment w stosunku do całkowitej kapitalizacji rynkowej ETH - Delphi Digital

Jedyna statystyka notująca drastyczny spadek to fundusze zebrane, w tym roku, za pomocą ICO. Wynika to w dużej mierze z tego, że rolę ICO przejęły IEO – sprzedaż tokenów nowych projektów za pomocą giełd kryptowalut.



Rysunek 23: Fundusze zebrane przez ICO na ETH

ICO posiadają w swoich skarbcach łącznie 2.6 miliona ETH.



Rysunek 24: Fundusze ICO na ETH

Wartość transakcji przesyłanych w ETH (mierząc w USD) pomimo spadku wyceny giełdowej Etheru w 2018 roku, utrzymuje się na stabilnym poziomie.

Rysunek 25: Wartość przesłanych transakcji mierzona w USD

Wszystkie te statystyki pokazują zdrowy wzrost zainteresowania projektem, a także rosnące realne wykorzystanie projektów z nowych sektorów jak np.: DeFi. Ethereum zajmuje drugie miejsce pod względem ogólnej aktywności sieci (na ogólną aktywność sieci składa się liczba transakcji, wolumen oraz kilka innych czynników), zaraz za Bitcoinem. Żadna ze statystyk nie mówi o zmniejszającym się zainteresowaniu lub migracją użytkowników do innych projektów – wręcz przeciwnie.

Konkurencja dla Ethereum

Hyperledger Fabric

Moim zdaniem, blockchain od IBM nie ma szans na ewolucję poza relatywnie małą, prywatną sieć dla wybranych organizacji. IBM wchodzący w kryptowaluty jest wszystkim, czego ta społeczność chciała uniknąć. Dzięki Fabric możemy tworzyć tokeny, ale tylko w ściśle określonych sytuacjach.

R3 Corda

Corda R3 to w rzeczywistości zaledwie oprogramowanie inspirowane blockchainem, przeznaczone głównie do zastosowań w sektorze bankowym. Cordzie brak jakichkolwiek cech decentralizacji, przez co nie można mówić o zaufaniu do sieci. Corda może wydawać tokeny, ale znów – jedynie w z góry określonych okolicznościach.

EOS

Jak już dyskutowano bez końca, platforma kontrolowana przez grupę 21 węzłów walidujących wszystkie transakcje to, najprościej mówiąc - shitcoin. Grupa może wejść w zmowę i cenzurować, jeśli sobie tego życzą. Rządy i inne dobrze zaopatrzone podmioty mogą ich przekupić lub zmusić do działania wbrew ich woli oraz przeciw dobru i bezpieczeństwu osób korzystających z platformy. Grupa ta jest w stanie odwrócić wcześniej wysłane transakcje[27], przez co nie ma mowy o jakimkolwiek zaufaniu i skutecznym wykorzystaniu tej kryptowaluty.

Początkowe założenie było takie, że jeśli producenci bloków zaczną działać przeciwko użytkownikom, zostaną poddani głosowaniu i finalnie pozbawieni swoich ról – to miał być punkt, w którym EOS stawał się zdecentralizowany. Niestety, nie ma dobrego sposobu na wykrycie, że węzły są w zmowie lub zostały uszkodzone, bądź zmuszone do niewłaściwego działania.

[27] EOS Reverses Transactions: https://cointelegraph.com/news/eos-reverses-previously-confirmed-transactions-as-pundits-decry-centralization

Cosmos

Nie sposób zaprzeczyć, że Cosmos tworzą solidni inżynierowie. Jednak Cosmos koncentruje się na umożliwieniu współdziałania różnych platform (cross-chain atomic swaps). I nie wydaje się, że w ciągu najbliższych kilku lat będzie istniała duża interoperacyjność między platformami, poza umożliwieniem tokenom przemieszczania się tam i z powrotem.

Dfinity

Ponieważ Dfinity jest obecnie zamkniętym systemem, kontrolowanym przez niewielką liczbę inwestorów i posiadaczy tokenów, nie biorę ich pod uwagę w tym zestawieniu. Jeśli kod źródłowy stanie się open-source, będę w stanie przeprowadzić osobną analizę.

Analiza ta coraz bardziej nakierowuje nas na jedno, ważne pytanie. Czy ktoś jest rzeczywiście w stanie zagrozić obecnej hegemonii Ethereum na rynku smart kontraktów, dApp i DeFi? Spójrzmy teraz na kilka niebezpiecznych scenariuszy, w których to Ethereum staje się ofiarą swego własnego sukcesu.

Zagrożenia dla projektu

- Wojna między górnikami, a deweloperami – konflikt mający na celu poważne opóźnienie migracji ETH na POS, aby górnictwo dalej było opłacalne.
- Nieokreślony MAX SUPPLY kryptowaluty.
- Wysoka inflacja w czasie wprowadzenia nagród z POS w Beacon Chain.
- Niemożność wprowadzenia technologii zakładanych w Roadmapie Serenity.
- Przeciążenie informacyjne sieci wraz ze wzrostem popularności projektu – opóźnienie rozwiązań zwiększających skalowalność sieci spowodować mogłoby poważne zapychanie się sieci.
- Utrzymanie sieci ETH 1.0 do czasu pełnego startu ETH 2.0.

Podsumowanie ETH 2.0

Zmiany jakie czekają Ethereum są interesujące. Jednak jakkolwiek nowa technologia, a także rosnące statystyki wykorzystania kryptowaluty by nas nie ekscytowały, należy wziąć pod uwagę możliwość dalszych opóźnień w pracach nad fundamentalnym protokołem oraz potencjalnych błędów. Scenariusz, w którym górnicy sabotują łańcuch, lub następuje niemożność określenia górnej granicy podaży Ethereum – choć może być to długofalowo zdrowe dla sieci i jej rozwoju, potencjalny inwestor musi mieć powyższe rzeczy na uwadze. Ethereum 2.0 czeka ciężki sprawdzian, podczas którego podstawowe siły ekonomiczne, jak i rynek, zweryfikują czy protokół gotowy jest na globalną adopcję. Ważne jest również to, aby cały czas pamiętać z jak eksperymentalną technologią mamy do czynienia. Mimo tego, bazując na wynikach raportu, uważam, że Ethereum utrzyma swoją miażdżącą dominację na rynku kryptowalut w stosunku do innych projektów oferujących możliwość programowania inteligentnych kontraktów. Żaden z projektów, które przedstawiane są jako konkurenci Ethereum, dotychczas nie wprowadził niczego, co mogłoby zagrozić statusowi ETH.

stokarz

Archiwum raportów:

Ambrosus (AMB)

https://ambrosus.pl/latwe-wejscie-w-blockchain-amb-net-masternode-system/

NEO (NEO)

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

Stellar (XLM)

https://www.docdroid.net/WS10r86/stellar-konsensus-raport-by-stokarz.pdf

LISK (LSK)

https://www.docdroid.net/1PCleep/lisk-lsk-raport-by-stokarz.pdf

Zcash (ZEC)

https://www.docdroid.net/LWYUZUu/zcash-zec-raport-by-stokarz.pdf

PUMP MY SHITCOIN – Edycja Lato 2019

https://www.docdroid.net/KxrcCJu/pump-my-shitcoin-lato-2019.pdf

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

https://t.me/TRQProAlty

https://t.me/CyberKryptoFreedomChat