Vitalik Buterin

Ważny głos w dyskusji na temat rozwoju nowej technologii, która wpłynie na losy wszystkich ludzi!
LAURA SHIN, autorka książki *The Cryptopians*

DOWÓD STAWKI

PROOF *of* STAKE

(PoS), powstanie Ethereum i filozofia łańcucha bloków

Helion onepress

Tytuł oryginału: Proof of Stake: The Making of Ethereum
and the Philosophy of Blockchains

Tłumaczenie: Krzysztof Krzyżanowski

ISBN: 978-83-289-0201-5

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://onepress.pl/user/opinie/dowsta
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *onepress@onepress.pl*
WWW:*https://onepress.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Rynki, instytucje i waluty — nowe źródło motywacji społecznej

„Bitcoin Magazine"

10 stycznia 2014 r.

Aż do tego momentu z problemem motywowania ludzi do produktywnych działań powiązane były dwie główne kategorie rozwiązań: rynki i instytucje. Rynki w swojej czystej formie są w pełni zdecentralizowane i składają się z niemal nieskończonej liczby podmiotów, które wchodzą ze sobą w indywidualne interakcje zmieniające na lepsze położenie obu zaangażowanych stron. Z kolei instytucje siłą rzeczy są hierarchiczne: dana instytucja ma jakieś władze, które decydują o tym, jaka aktywność będzie najbardziej użyteczna w takim czy innym okresie, a następnie określają nagrodę pozwalającą zachęcić ludzi do takich wysiłków. Dzięki centralizacji instytucja może motywować poszczególne osoby do tworzenia dóbr publicznych zapewniających korzyści tysiącom lub wręcz milionom ludzi, nawet jeżeli zyski z perspektywy pojedynczej osoby są bardzo skromne. Nie możemy jednak zapominać o powszechnie znanym problemie: centralizacji towarzyszy też szereg zagrożeń. Przez ostatnich 10 tysięcy lat te dwie opcje były zasadniczo wszystkim, co mieliśmy do dyspozycji. Wraz z pojawieniem się bitcoina i jego pochodnych ten stan rzeczy może się wszakże zmienić — niewykluczone, że jesteśmy właśnie świadkami narodzin trzeciego źródła motywacji: walut.

DRUGA STRONA MONETY

Jeżeli spojrzeć z typowej perspektywy, waluta pełni w społeczeństwie trzy kluczowe funkcje. Służy jako środek wymiany, pozwalając ludziom kupować i sprzedawać dobra w zamian za pieniądze (dzięki temu nie musisz się ograniczać do handlu wymiennego i szukać kogoś, kto dysponuje dokładnie tym, czego szukasz, a zarazem próbuje zapewnić sobie to, co znajduje się w Twoim posiadaniu). Stanowi też nośnik wartości, pozwalając ludziom tworzyć i konsumować dobra w różnym tempie. Oprócz tego jest środkiem służącym do określania wartości — miarą, której ludzie mogą użyć, żeby określać stałą „wielkość produkcji". Wiele osób może jednak nie zdawać sobie sprawy z tego, że waluty mają też czwartą funkcję, której znaczenie pozostawało przez większość czasu ukryte: mam tu na myśli seniorat.

Seniorat można formalnie zdefiniować jako różnicę między rynkową wartością waluty a jej faktyczną wartością — czyli wartością, jaką miałaby waluta, gdyby nikt nie używał jej jako środka płatniczego. W przypadku pradawnych walut w rodzaju zboża ta różnica wynosiła zasadniczo zero. Gdy jednak rynki ekonomiczne i waluty stawały się coraz bardziej złożone, ta „fikcyjna wartość" generowana na pozór znikąd przez pieniądze stawała się coraz większa. Ostatecznie doszło do sytuacji, w której w przypadku większości współczesnych walut w rodzaju dolara czy bitcoina seniorat stanowi całą wartość waluty.

Co się jednak dzieje z tymi środkami? W przypadku walut, które opierają się na naturalnych zasobach w rodzaju złota, większość wartości jest po prostu trwoniona. To, że każdy gram złota może w ogóle zaistnieć, jest następstwem wysiłków górnika, który wydobył ten kruszec. Początkowo część górników czerpie korzyści ze swojej pracy, ale na rynku efektywnym wszystkie łatwe sposobności do zarobku szybko znikają, a koszty produkcji osiągają poziom zbliżony do zysków. Istnieją oczywiście sprytne rozwiązania, dzięki którym złoto może zapewniać dochody związane z senioratem; za dawnych czasów królowie bili na przykład złote monety, które były warte więcej niż zwyczajne złoto — takim monetom towarzyszyła domniemana obietnica króla, który był gwarantem ich autentyczności. W ogólnym ujęciu generowana w ten sposób wartość nie trafiała jednak w ręce konkretnej osoby. W przypadku dolara amerykańskiego widać pewien postęp

w tej sferze: część dochodów związanych z senioratem zasilała budżet władz państwowych. Na wiele sposobów był to wyraźny krok naprzód, ale rewolucja pozostawała niedokończona — chociaż walucie towarzyszyły teraz korzyści związane ze scentralizowanym senioratem, w ślad za nimi pojawiły się też zagrożenia wynikające z silnych więzi łączących pieniądz z jedną z największych scentralizowanych instytucji, jakie powstały w całej historii ludzkości.

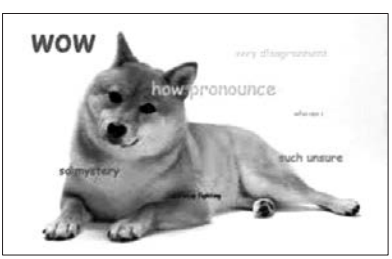
NA RYNKU POJAWIA SIĘ BITCOIN

Pięć lat temu pojawił się nowy rodzaj pieniądza, bitcoin. Przypomina on dolara w tym sensie, że całą wartość tej waluty stanowi seniorat. Bitcoin jako taki nie ma swojej naturalnej, wewnętrznej wartości. Jak wykorzystywane są jednak te środki pozyskane za sprawą senioratu? Część z nich trafia w ręce górników jako zysk, natomiast reszta pokrywa wydatki górników — koszty związane z zapewnianiem bezpieczeństwa sieci Bitcoin. Mamy tu zatem do czynienia z walutą, w przypadku której zyski z senioratu przeznaczane są bezpośrednio na finansowanie dobra publicznego, a konkretniej bezpieczeństwa sieci Bitcoin. Znaczenie tego mechanizmu jest powszechnie niedoceniane: to rozwiązanie motywujące, które jest zdecentralizowane, nie wymaga żadnej władzy ani kontroli i tworzy dobra publiczne — a wszystko to dzięki ulotnej „fikcyjnej wartości" powstającej dzięki temu, że ludzie używają bitcoina jako środka wymiany i rozwiązania umożliwiającego przechowywanie majątku.

Nieco później pojawiło się inne rozwiązanie — primecoin, czyli pierwsza waluta, która miała wykorzystywać zyski z senioratu z myślą o realizacji jakiegoś użytecznego zewnętrznego celu: zamiast zmuszać górników do wyliczania (w ostatecznym rozrachunku bezużytecznych) haszów SHA256, primecoin zachęca te osoby do wyszukiwania łańcuchów Cunninghama składających się z liczb pierwszych. Wspiera tym samym bardzo wąską kategorię nauk obliczeniowych i motywuje twórców komputerów do szukania metod pozwalających optymalizować układy scalone pod kątem obliczeń arytmetycznych. Wartość tej kryptowaluty szybko wzrosła, a primecoin znajduje się aktualnie w grupie 11 najpopularniejszych kryptowalut — choć najważniejsza korzyść praktyczna, jaką zapewnia indywidualnemu

użytkownikowi, a więc czas wydobycia bloku wynoszący 60 sekund, jest wspólnym mianownikiem wielu innych, dużo mniej znanych kryptowalut.

W grudniu — a więc kilka miesięcy później — byliśmy świadkami nagłego wzrostu popularności waluty, która jest jeszcze bardziej osobliwa, a jej sukces stanowi jeszcze większe zaskoczenie: mam na myśli dogecoina, znanego też pod nazwą „pieseł". Dogecoin, oznaczony symbolem DOGE, to waluta, która od strony technicznej jest niemal idealną kopią litecoina — jedyną różnicą jest to, że maksymalna liczba monet wynosi nie 84 miliony, a 100 miliardów. Niezależnie od tego faktu ta nowa waluta osiągnęła kapitalizację rynkową przekraczającą 14 milionów dolarów, plasując się pod tym względem na szóstym miejscu w rankingu kryptowalut. Wspominano o niej także na łamach czasopism „Business Insider" i „Vice". Na czym polega jej wyjątkowość? Zasadniczo bazuje na internetowym memie. „Doge", czyli slangowe określenie psa, które po raz pierwszy pojawiło się w 2005 r. w serialu animowanym *Homestar Runner*, stało się z czasem globalnym fenomenem, a ludzie zaczęli umieszczać krótkie stwierdzenia zapisane w rozmaitych kolorach fontem Comic Sans na tle fotografii psa rasy shiba inu. Ten mem stanowi podstawę całego brandingu dogecoina: wszystkie jego witryny społecznościowe i fora — włącznie z oficjalną stroną dogecoina, obowiązkowym wątkiem zakładanym na forum Bitcointalk po stworzeniu nowej kryptowaluty[2], a także subredditami /r/dogecoin i /r/dogecoinmarkets — są przyozdobione grafikami, na których widoczny jest charakterystyczny czworonóg. To wystarczyło, żeby kopia litecoina osiągnęła kapitalizację rynkową przewyższającą 14 milionów dolarów.



[2] W tamtym okresie serwis Bitcointalk był najważniejszym forum dyskusyjnym poświęconym kryptowalutom. Jego założycielem był Satoshi Nakamoto. Każda nowa kryptowaluta miała na forum swój własny wątek.

Trzeci przykład pochodzi spoza świata kryptowalut — jest nim ven, czyli bardziej tradycyjna, scentralizowana waluta, której podstawą jest koszyk dóbr obejmujący towary, waluty i kontrakty terminowe futures. Twórcy vena dodali niedawno do swojego koszyka kontrakty terminowe na emisję CO_2, tworząc tym samym pierwszą walutę, która jest w jakiś sposób „powiązana ze środowiskiem". W istocie za tym posunięciem kryje się sprytna ekonomiczna zagrywka: wspomniane kontrakty terminowe są powiązane z walutą w negatywny sposób, tak więc jej wartość rośnie w miarę, jak społeczeństwo odchodzi od rozwiązań generujących dużo CO_2, a kontrakty na emisję CO_2 stają się mniej zyskowne. To oznacza, że każda osoba posiadająca walutę ven jest teraz subtelnie motywowana ekonomicznie do tego, żeby wspierać bardziej ekologiczne zachowania, a część zainteresowania tą walutą wynika właśnie z opisywanej tu kwestii.

Ogólnie rzecz biorąc, wszystkie te przykłady pokazują, że alternatywne waluty są zasadniczo w pełni zależne od marketingu oddolnego, który pozwala zadbać o ich popularyzację: nikt nie kupuje bitcoinów, primecoinów, dogecoinów czy waluty ven od domokrążców czy wybitnych sprzedawców zdolnych przekonać daną osobę do takiego czy innego rozwiązania. Oprócz tego to nie tylko techniczna wyższość danej waluty decyduje o tym, czy zdobędzie ona popularność — równie istotną kwestią są ideały. To właśnie ideały kryjące się za bitcoinem doprowadziły do tego, że jest on akceptowany przez bramki płatności na stronach wykorzystujących WordPressa, przez serwis Mega, a teraz także przez firmę Overstock. Zapewne to właśnie z tych samych powodów kryptowaluta ripple, choć od strony technicznej byłaby z perspektywy sprzedawców lepszym rozwiązaniem od bitcoina (istotne jest zwłaszcza to, że transakcje potwierdzane są już po pięciu sekundach), nie zdobyła jak na razie zbyt wielkiej popularności: ponieważ jest to połowicznie scentralizowany protokół wspierany przez firmę, która przejęła 100 procent wyemitowanej waluty, całe to rozwiązanie siłą rzeczy jest nieatrakcyjne z perspektywy wielu entuzjastów kryptowalut, którzy dążą do sprawiedliwości i decentralizacji. W tym momencie to właśnie ideały primecoina i dogecoina — wspieranie odpowiednio nauki i dobrej zabawy — umożliwiają funkcjonowanie obu tych walut.

KRYPTOWALUTY JAKO ELEMENT EKONOMICZNEJ DEMOKRACJI

Cztery przywołane powyżej przykłady zapewniają nam wraz z koncepcją fikcyjnej wartości generowanej przez seniorat coś, co może się potencjalnie przerodzić w podstawy nowej odmiany „ekonomicznej demokracji": możemy tworzyć nowe waluty, w przypadku których zyski płynące z senioratu lub emisji pozwolą wspierać określone sprawy, a ludzie będą mogli głosować na te kwestie, akceptując określone waluty w swojej działalności biznesowej. Jeśli ktoś nie ma własnej firmy, może się zaangażować w wysiłki marketingowe i zachęcać przedsiębiorców do akceptacji takiej czy innej waluty. Ktoś może stworzyć socialcoina — walutę, która co miesiąc będzie zapewniać tysiąc jednostek każdej osobie na świecie, a jeśli ta koncepcja spodoba się wystarczająco dużej liczbie ludzi i zaczną oni akceptować tę walutę, dojdzie do narodzin obywatelskiego programu dywidendowego, który nie będzie wymagał scentralizowanego finansowania. Możemy też powoływać do życia waluty, które będą wspierać badania medyczne, eksplorację kosmosu lub świat sztuki; w istocie rozmaici artyści, twórcy podcastów i muzycy rozważają aktualnie koncepcję tworzenia własnych walut, które posłużą dokładnie takim celom.

Jeśli chodzi o specyficzną kategorię dóbr publicznych, czyli badania związane z naukami obliczeniowymi, możemy tak naprawdę pójść o krok dalej i zadbać o zautomatyzowanie procesu dystrybucji. Nauki obliczeniowe można byłoby wspierać za sprawą mechanizmu, który nie doczekał się jeszcze szerokiego wykorzystania w prawdziwym świecie, ale został przedstawiony w formie teoretycznej koncepcji przez twórcę peercoina i primecoina, Sunny'ego Kinga. Mam tu na myśli coś, co określane jest mianem *proof of excellence*, czyli dowodu doskonałości. Koncepcja kryjąca się za tym pomysłem sprowadza się do tego, że udział danej osoby w zdecentralizowanej puli głosów i nagroda tej osoby nie są powiązane z mocą obliczeniową jej urządzeń czy liczbą posiadanych monet, ale z umiejętnością rozwiązywania złożonych problemów matematycznych i algorytmicznych, które mogą zapewnić korzyści całej ludzkości. Gdyby ktoś chciał na przykład wspierać badania nad teorią liczb, mógłby wkomponować w daną walutę zadania dotyczące rozkładania na czynniki pierwsze liczb RSA, a waluta zapewniałaby automatycznie 50 tysięcy jednostek (plus być może prawo głosu dotyczące

poprawności wykopywanych bloków) pierwszej osobie, która podałaby rozwiązanie takiego problemu. W teorii coś takiego mogłoby się nawet stać standardowym elementem modelu emisji dowolnej waluty.

Oczywiście, koncepcja wykorzystywania w ten sposób walut nie jest niczym nowym; „waluty społecznościowe" o zasięgu lokalnym były w użytku od ponad stu lat. W ostatnich dekadach traciły jednak na popularności w stosunku do początków XX w., kiedy to cieszyły się największym zainteresowaniem. Taki stan rzeczy wynikał głównie z ich bardzo ograniczonego zasięgu; oprócz tego nie mogły też czerpać korzyści z wysoce efektywnego systemu bankowego powiązanego z szerzej wykorzystywanymi walutami w rodzaju dolara amerykańskiego. Wraz z pojawieniem się kryptowalut te problemy zostały jednak błyskawicznie rozwiązane: kryptowaluty siłą rzeczy mają globalny charakter i odwołują się do potężnego, cyfrowego systemu bankowego zintegrowanego z ich kodem źródłowym. To oznacza, że być może nadszedł właśnie odpowiedni moment na tryumfalny powrót walut społecznościowych, które dzięki nowym rozwiązaniom technologicznym mogłyby odgrywać dużo istotniejszą rolę niż w XIX i XX w., stając się ważnym, mainstreamowym elementem światowej gospodarki.

Co czeka nas w takim razie w przyszłości? Dogecoin pokazał już wszystkim zainteresowanym, jak łatwo jest stworzyć własną walutę: jeden z deweloperów bitcoina, Matt Corallo, stworzył bardzo niedawno witrynę *coingen.io*, która służy wyłącznie do szybkiego tworzenia klonów bitcoina lub litecoina z nieznacznie zmodyfikowanymi parametrami. Nawet jeżeli liczba dostępnych opcji jest aktualnie dosyć ograniczona, strona cieszy się sporą popularnością — doprowadziła już do powstania setek walut, i to pomimo faktu, że trzeba za coś takiego zapłacić 0,05 BTC. Gdy serwis Coingen pozwoli użytkownikom na wykorzystywanie mechanizmu dowodu doskonałości, umożliwi przekazywanie części zysków z emisji określonej organizacji lub fundacji i zapewni więcej opcji dotyczących własnego brandingu, możemy się spodziewać narodzin tysięcy kryptowalut, które będą potem wykorzystywane w internecie. Czy te waluty sprawdzą się jako bardziej zdecentralizowana i demokratyczna metoda tworzenia puli finansowych i wspierania projektów publicznych lub działań, które pozwolą stworzyć społeczeństwo, o jakim marzymy? Może tak, może nie. Jeśli jednak wziąć pod uwagę, że niemal każdego dnia pojawia się jakaś nowa kryptowaluta, niewykluczone, iż już wkrótce poznamy odpowiedź na to pytanie.

Ethereum — waluta nowej generacji i platforma dla zdecentralizowanych aplikacji

„Bitcoin Magazine"

23 stycznia 2014 r.

Miniony rok okazał się okresem, w którym coraz częściej dochodziło do dyskusji na temat tak zwanych protokołów Bitcoin 2.0 — sieci kryptograficznych, które są inspirowane Bitcoinem, ale mają w zamyśle wykorzystywać swoje rozwiązania technologiczne w sposób wykraczający zdecydowanie poza świat walut. Najwcześniejszą implementacją tego pomysłu był namecoin, czyli przypominająca bitcoina waluta, która została stworzona w 2010 r. i mogła służyć do rejestrowania w zdecentralizowany sposób domen. Ostatnio na rynku pojawiły się również kolorowane monety (ang. *colored coins*), które pozwalają użytkownikom tworzyć własne waluty odwołujące się do sieci Bitcoin. Kolejnym rozwiązaniem są bardziej zaawansowane protokoły, takie jak Mastercoin, BitShares czy Counterparty, które mają oferować dostęp do instrumentów pochodnych, portfeli inwestycyjnych czy zdecentralizowanych giełd kryptowalut. Jak na razie wszystkie powstające protokoły tego typu były jednak wyspecjalizowane i albo miały za zadanie zapewniać specyficzne zestawy funkcjonalności dopasowane do potrzeb konkretnych branż, albo skupiały się na zastosowaniach o charakterze finansowym. W tym momencie grupa deweloperów (do której sam się zaliczam) postanowiła zainicjować projekt zmierzający w przeciwnym

kierunku: chodzi o stworzenie sieci kryptowalutowej, która byłaby tak uniwersalna, jak to tylko możliwe. Zapewniałaby ona podstawy, na których każdy mógłby budować wyspecjalizowane aplikacje służące do realizacji niemal dowolnych celów. Cały ten projekt nosi nazwę Ethereum.

PROTOKOŁY KRYPTOWALUT PRZYPOMINAJĄ CEBULE…

Wspólne założenie łączące wiele protokołów kryptowalut 2.0 sprowadza się do koncepcji, w myśl której kryptowaluty (podobnie zresztą jak internet) będą działały najlepiej, jeśli protokoły zostaną podzielone na różne warstwy. Jeżeli przyjmiemy ten tok rozumowania, Bitcoin może być uznawany za swoisty odpowiednik protokołu TCP/IP w ekosystemie kryptowalut, a kolejne protokoły nowej generacji można będzie budować na fundamentach zapewnianych przez Bitcoina, co przypominałoby istniejące aktualnie protokoły: SMTP wykorzystywany przez pocztę elektroniczną, HTTP używany przez strony internetowe czy XMPP stosowany w komunikatorach. Wszystkie one nałożone są na bazowy protokół TCP umożliwiający przesyłanie danych.

Jak na razie trzy główne protokoły wpisujące się w ten model to kolorowane monety, Mastercoin i Counterparty. Zasada funkcjonowania protokołu kolorowanych monet jest prosta. Żeby w ogóle je stworzyć, użytkownik opatruje określone bitcoiny specyficznym tagiem, nadając im tym samym szczególne znaczenie. Jeśli na przykład Bob jest emitentem złota, może mu zależeć na opatrzeniu pewnej liczby bitcoinów określonym tagiem i zakomunikowaniu, że każde satoshi odpowiada 0,1 grama złota, które będzie można u niego odebrać. Protokół śledzi potem te bitcoiny w łańcuchu bloków, co pozwala ustalić, kto jest w danym momencie ich właścicielem.

Mastercoin i Counterparty funkcjonują w nieco bardziej abstrakcyjny sposób: wykorzystują blockchain Bitcoina do przechowywania danych, tak więc transakcja Mastercoin lub Counterparty jest transakcją bitcoinową, aczkolwiek poszczególne protokoły interpretują te transakcje w odmienny sposób. Możemy zestawić ze sobą dwie transakcje mastercoinowe: jedna będzie oznaczała przesłanie 1 MSC, a druga — 100 tysięcy MSC. Z perspektywy użytkownika Bitcoina, który nie zna zasad funkcjonowania protokołu

Mastercoina, obydwie wyglądają jednak na drobne transakcje sprowadzające się do przesłania 0,0006 BTC. Metadane powiązane z Mastercoinem zakodowane są w danych wyjściowych transakcji. Klient Mastercoina musi potem przeszukać łańcuch bloków Bitcoina pod kątem transakcji mastercoinowych, żeby określić aktualny bilans tej waluty.

Miałem okazję bezpośrednio rozmawiać z wieloma osobami odpowiedzialnymi za stworzenie protokołów kolorowanych monet i Mastercoina; oprócz tego byłem zaangażowany w rozwijanie obu tych projektów. Po mniej więcej dwóch miesiącach zgłębiania tych kwestii i udziału w tych inicjatywach uświadomiłem sobie jednak, że chociaż sama koncepcja stworzenia takich wysokopoziomowych protokołów bazujących na rozwiązaniach niskopoziomowych jest jak najbardziej słuszna, to istniejące dziś implementacje tego pomysłu są bardzo niedoskonałe, przez co w swoim aktualnym kształcie mogą one nigdy nie zdobyć większej popularności.

Powodem nie jest wcale to, że idee kryjące się za tymi protokołami skrywają jakieś wady. Owe pomysły są w istocie fantastyczne, a już sama reakcja społeczności świadczy o tym, że są to wysiłki zmierzające do zrobienia czegoś, co jest bardzo potrzebne. Sęk w tym, że niskopoziomowy protokół, na którym mają bazować te wysokopoziomowe rozwiązania — protokół Bitcoina — nie jest po prostu stworzony do czegoś takiego. Nie próbuję przez to powiedzieć, że Bitcoin jest nieudanym rozwiązaniem lub nie zasługuje na miano rewolucyjnego wynalazku. Jako protokół służący do przechowywania i przekazywania środków finansowych Bitcoin sprawdza się znakomicie. Jeśli jednak szukamy efektywnego protokołu niskopoziomowego, Bitcoin okazuje się mniej wydajny. Nie przypomina TCP, na który można nałożyć kolejną warstwę w postaci HTTP; Bitcoina można raczej porównać do SMTP, czyli protokołu, który jest świetnym rozwiązaniem w kontekście określonego zadania (w przypadku SMTP jest to obsługa e-maili; w przypadku Bitcoina — realizacja transakcji finansowych), ale nie będzie zbyt dobry jako podstawa wszystkich innych rzeczy.

Opisywana tu niewydolność Bitcoina dotyczy zwłaszcza jednej kwestii: skalowalności. Sam Bitcoin jest tak skalowalny, jak to tylko możliwe w przypadku kryptowaluty; nawet gdyby łańcuch bloków osiągnął rozmiary przekraczające 1 terabajt, w białej księdze Bitcoina opisano protokół, który nosi miano „uproszczonej weryfikacji płatności". Sprawia on, że „lekki klient",

który dysponuje skromną przestrzenią na dane i łączem o przepustowości wynoszącej zaledwie kilka megabajtów, jest w stanie dokonać w bezpieczny sposób oceny tego, czy dotarły do niego jakieś transakcje. W przypadku kolorowanych monet czy Mastercoina ta możliwość jednak znika. Powód jest prosty: jeśli chcesz określić barwę kolorowanej monety, nie wystarczy, że użyjesz uproszczonej weryfikacji płatności, która dowiedzie istnienia takiej monety — musisz jeszcze prześledzić jej losy aż do momentu jej powstania oraz przeprowadzić uproszczoną weryfikację płatności każdej zrealizowanej po drodze operacji. Czasami taka analiza wcześniejszych kroków okazuje się bardzo złożona, a w przypadku protokołów metacoinowych nie sposób dojść do czegokolwiek bez weryfikacji każdej z tych transakcji.

Dokładnie ten problem ma rozwiązać Ethereum. Nie ma być wcale odpowiednikiem szwajcarskiego scyzoryka w świecie protokołów — nie próbuje też zapewniać setek różnych funkcjonalności dopasowanych do wszelkich możliwych potrzeb. Ma jednak stanowić doskonały protokół bazowy, który będzie można wykorzystywać zamiast Bitcoina jako podstawę funkcjonowania innych zdecentralizowanych aplikacji, zapewniając im więcej narzędzi, a także pozwalając czerpać korzyści ze skalowalności i wydajności Ethereum.

KONTRAKTY — NIE TYLKO NA RÓŻNICĘ KURSOWĄ

W czasie, gdy trwały prace nad Ethereum, spore zainteresowanie budziła kwestia wykorzystywania kryptowalut do zawierania kontraktów finansowych — podstawową odmianą takiego instrumentu pochodnego jest kontrakt na różnicę kursową (ang. *contract for difference*, w skrócie CFD). W przypadku takiego kontraktu dwie strony zgadzają się zainwestować taką samą kwotę, a potem podzielić się środkami w proporcjonalny sposób zależny od wartości aktywów będących podstawą danego kontraktu. W ramach przykładowego CFD Alice i Bob mogą wyłożyć po 1000 dolarów — po 30 dniach łańcuch bloków automatycznie zwróci Alice 1000 dolarów plus 100 dolarów za każdego dolara, o którego wzrósł w tym czasie kurs LTC/USD, natomiast Bob otrzyma resztę pieniędzy. Takie kontrakty

umożliwiają spekulację aktywami odwołującą się do dużej dźwigni, choć mogą też chronić przed niestabilnością kursów kryptowalut, zmniejszając ryzyko finansowe — i to wszystko bez konieczności korzystania z jakiejkolwiek scentralizowanej giełdy.

Na tym etapie omawiania tej kwestii widać jednak wyraźnie, że kontrakty na różnicę kursową są tak naprawdę dosyć szczególnym przypadkiem wliczanym do dużo bardziej ogólnej kategorii kontraktów powiązanych z różnymi wzorami. Zamiast pobierać *x* dolarów od Alice i *y* dolarów od Boba, a potem zwracać Alice kwotę *x* dolarów powiększoną o dodatkowe *z* dolarów za każdego dolara, o którego wzrósł jakiś kurs, kontrakt powinien mieć możliwość przesłania Alice kwoty wyliczonej na podstawie jakiegokolwiek wzoru, co pozwalałoby zawierać kontrakty o dowolnej złożoności. Gdyby wzór pozwalał na użycie jako danych wejściowych liczb losowych, takich uogólnionych CFD można byłoby nawet użyć do zaimplementowania czegoś w rodzaju hazardu *peer-to-peer*.

Ethereum odwołuje się do tej koncepcji, po czym idzie o krok dalej. Kontrakty nie stanowią już umów, które są zawierane między dwiema stronami i mają określone daty rozpoczęcia i zakończenia — w świecie Ethereum są swego rodzaju autonomicznym podmiotem, którego istnienie jest symulowane przez łańcuch bloków. Każdy kontrakt Ethereum zawiera własny, wewnętrzny kod, który został zapisany w postaci skryptów i jest aktywowany za każdym razem, gdy ktoś zrealizuje jakąś transakcję, wykorzystując adres kontraktu. Język skryptowy ma dostęp do informacji na temat wartości transakcji, jej nadawcy i zawartości opcjonalnych pól danych, a także do niektórych danych bloku i pamięci wewnętrznej. Może wykorzystywać to wszystko jako dane wejściowe, a oprócz tego może realizować transakcje. Żeby zawrzeć CFD, Alice musiałaby stworzyć kontrakt i zasilić go równowartością 1000 dolarów w kryptowalucie. Później musiałaby zaczekać, aż Bob zaakceptuje kontrakt, również przesyłając środki o wartości 1000 dolarów. Kontrakt byłby zaprogramowany w taki sposób, żeby uruchomić w takiej sytuacji odliczanie. Po 30 dniach Alice lub Bob mogliby zrealizować niewielką transakcję, żeby znów aktywować kontrakt i uwolnić środki.

Oto przykład kodu kontraktu Ethereum na kurs waluty napisanego w języku wysokopoziomowym:

```
if tx.value < 100 * block.basefee:
 stop
if contract.memory[1000]:
 from = tx.sender
 to = tx.data[0]
 value = tx.data[1]
 if to <= 1000:
 stop
 if contract.memory[from] < value:
 stop
 contract.memory[from] = contract.memory[from] - value
 contract.memory[to] = contract.memory[to] + value
else: contract.memory[mycreator] = 10000000000000000
contract.memory[1000] = 1
```

Jeśli nie liczyć tego specyficznego modelu kontraktu na różnicę kursową, biała księga opisuje wiele innych typów transakcji, które będzie można realizować dzięki skryptom Ethereum. Oto kilka pozycji z tej listy:

- **Depozyty zabezpieczone wieloma kluczami:** Przypominają one usługę arbitrażową Bitrated powiązaną z Bitcoinem, aczkolwiek mają bardziej skomplikowane zasady. Nie będzie na przykład konieczności ręcznego przesyłania przez sygnatariuszy częściowo podpisanych transakcji; poszczególne osoby będą mogły jedna po drugiej asynchronicznie autoryzować za pomocą łańcucha bloków wycofanie środków, a transakcja zostanie automatycznie sfinalizowana, gdy zbierze się wystarczająco duża liczba takich potwierdzeń.
- **Rachunki oszczędnościowe:** Jedno z ciekawych rozwiązań mogłoby funkcjonować w następujący sposób — przyjmijmy, że Alice planuje przechować gdzieś sporą kwotę, ale nie chce ryzykować utraty tych środków, gdyby jej klucz prywatny został ukradziony lub zgubiony. Zawiera kontrakt z Bobem, budzącym pewne zaufanie bankierem. Zgodnie z zasadami tego układu Alice może wypłacić maksymalnie 1 jednostkę waluty w ciągu dnia, Alice za zgodą Boba może wypłacić dowolną kwotę, natomiast sam Bob może wypłacić maksymalnie 0,05 jednostki dziennie. W normalnych okolicznościach Alice potrzebuje

tylko niewielkich kwot, a gdyby potrzebowała większej sumy pieniędzy, może potwierdzić przed Bobem swoją tożsamość i dokonać wypłaty środków. Gdyby doszło do kradzieży klucza prywatnego Alice, kobieta może skontaktować się z Bobem i przenieść środki na inny kontrakt, zanim złodziej zdoła wypłacić więcej niż 1 jednostkę. Jeżeli Alice utraci swój klucz prywatny, Bob będzie w stanie pomóc jej w odzyskaniu środków. Gdyby z kolei Bob okazał się niegodny zaufania, Alice może wypłacać środki 20 razy szybciej niż on. Krótko mówiąc, mamy tu do czynienia z bezpieczeństwem zapewnianym przez tradycyjną bankowość, ale nie musimy okazywać prawie żadnego zaufania.

- **Hazard *peer-to-peer*:** Ethereum może posłużyć jako podstawa do zaimplementowania wszelkich protokołów związanych z hazardem *peer-to-peer*. Bardzo proste rozwiązanie mogłoby się ograniczać do kontraktu na różnicę dotyczącego losowych danych takich jak hasz jakiegoś bloku.
- **Tworzenie własnych walut:** Wykorzystanie wewnętrznej pamięci Ethereum pozwala tworzyć w ramach tej platformy całkowicie nowe waluty. Mogłyby one być skonstruowane w taki sposób, żeby wchodzić we wzajemne interakcje i zapewniać zdecentralizowane mechanizmy wymiany lub inne zaawansowane funkcjonalności.

Na tym polega właśnie przewaga kodu Ethereum: ponieważ język skryptowy jest zaprojektowany w taki sposób, żeby nie narzucać żadnych ograniczeń (jeśli nie liczyć systemu opłat), pozwala zakodować praktycznie dowolne zasady. Nic nie stoi na przykład na przeszkodzie, żeby przenieść do łańcucha bloków zarządzanie firmowymi oszczędnościami i stworzyć kontrakt, zgodnie z którym jakikolwiek większy transfer środków będzie możliwy dopiero wtedy, gdy zaakceptuje go 60 spośród aktualnych akcjonariuszy firmy (a za zgodą mniejszej grupy, liczącej chociażby 30 osób, możliwy będzie transfer maksymalnie 1 jednostki waluty). Można też tworzyć inne struktury, które nie będą tak kapitalistyczne w tradycyjnym rozumieniu tego słowa; jedną z koncepcji jest powołanie do życia demokratycznej organizacji, w której obowiązywałaby tylko jedna zasada: przyjęcie do tej grupy nowej osoby byłoby możliwe wyłącznie w sytuacji, w której zgodziłyby się na to dwie trzecie jej aktualnych członków.

NA FINANSACH ŚWIAT SIĘ NIE KOŃCZY

Zastosowania finansowe stanowią zaledwie wąski wycinek tego, co można zrobić za pomocą Ethereum i nałożonych na te podstawy protokołów kryptograficznych. Chociaż to właśnie zastosowania finansowe Ethereum mogą być tym, co wzbudzi początkową ekscytację wielu osób związanych ze społecznością kryptowalutową, długoterminowy potencjał tego projektu kryje się niewątpliwie w sposobach, w jakie Ethereum może współpracować z innymi, niefinansowymi protokołami *peer-to-peer*. Jednym z głównych problemów trapiących takie protokoły był dotychczas brak zachęt — w przeciwieństwie do scentralizowanych platform dążących do wypracowania zysku tutaj brakowało finansowych argumentów przemawiających za uczestnictwem w danej inicjatywie. W niektórych przypadkach nagrodą może być już samo zaangażowanie w taki projekt; to właśnie z tego powodu ludzie nadal tworzą oprogramowanie *open source*, redagują artykuły na Wikipedii i publikują komentarze na forach czy wpisy na blogach. Jeśli jednak chodzi o protokoły *peer-to-peer*, udział w takich inicjatywach nie jest najczęściej „przyjemną" aktywnością w jakimkolwiek głębszym sensie — sprowadza się raczej do poświęcenia dużej ilości zasobów, utrzymywania w tle aktywnego demona (który może potencjalnie stanowić obciążenie dla procesora czy baterii) i zapomnienia o całej sprawie.

Od dawna istnieją na przykład protokoły dystrybucji danych takie jak Freenet, które zapewniają zasadniczo każdemu użytkownikowi zdecentralizowany, niepodlegający cenzurze hosting statycznych stron internetowych. W praktyce okazuje się jednak, że Freenet jest bardzo wolny, a mało kto wspiera tę inicjatywę swoimi zasobami. Protokoły wykorzystywane do udostępniania plików zmagają się ze wspólnym problemem: chociaż altruizm jest wystarczającą motywacją do rozpowszechniania popularnych przebojów kasowych, okazuje się dużo mniej skuteczny, gdy w grę wchodzą materiały, które nie wpisują się w mainstreamowe preferencje. To oznacza, że współdzielenie plików *peer-to-peer* paradoksalnie może nie tyle osłabiać, ile wspierać centralizację w świecie rozrywki i mediów. Wszystkie te problemy mogą jednak potencjalnie zostać rozwiązane, jeśli wprowadzimy czynnik motywujący i sprawimy, że zaangażowanie w funkcjonowanie sieci

będzie pozwalało tworzyć nie tylko realizowane w wolnym czasie projekty non profit, ale także firmy czy inicjatywy, dzięki którym ludzie będą mogli zarabiać na życie.

- **Odpłatne udostępnianie przestrzeni dyskowej:** Tę koncepcję można zasadniczo porównać do zdecentralizowanego Dropboksa. Cały ten pomysł działałby w następujący sposób: gdyby użytkownik chciał, żeby plik o rozmiarach 1 GB został przechowany w sieci, mógłby stworzyć z tych danych strukturę określaną mianem drzewa Merkle'a. Kolejne kroki polegałyby na umieszczeniu korzenia tego drzewa wraz z 10 jednostkami eteru w kontrakcie i przesłaniu pliku do innej wyspecjalizowanej sieci, której węzły są gotowe udostępniać swoją przestrzeń dyskową i nasłuchują takich wiadomości. Każdego dnia kontrakt automatycznie wybierałby losową gałąź drzewa (np. „lewo → prawo → lewo → lewo → lewo → prawo → lewo") kończącą się jakimś blokiem wchodzącym w skład pliku, a potem przyznawałby 0,01 jednostki eteru pierwszemu węzłowi, który dostarczyłby te dane. Węzły przechowywałyby w takiej sytuacji cały plik, żeby zwiększyć prawdopodobieństwo otrzymania nagrody.
- **Bitmessage i Tor:** Bitmessage to protokół e-mail nowej generacji, który jest zarówno w pełni zdecentralizowany, jak i zaszyfrowany, co pozwala na bezpieczne wysyłanie wiadomości do innych użytkowników Bitmessage bez konieczności polegania na stronach trzecich (jeśli nie liczyć samej sieci). Bitmessage ma jednak poważną wadę, która odbija się na użyteczności tego rozwiązania: zamiast wysyłać wiadomości na łatwy do zapamiętania adres w rodzaju *mojenazwisko@email*, musisz używać dziwacznych adresów Bitmessage, składających się z ciągu 34 znaków (np. *BM-BcbRqcFFSQUUmXFKsPJgVQPSiFA3Xash*). Dzięki kontraktom Ethereum można rozwiązać ten problem: użytkownicy mogą się zarejestrować w specjalnym kontrakcie Ethereum, a klient Bitmessage może przeszukać łańcuch bloków Ethereum, żeby znaleźć 34-znakowy adres Bitmessage powiązany z takim czy innym użytkownikiem. Sieć anonimizująca Tor zmaga się z tym samym problemem, w związku z czym też mogłaby skorzystać na opisanym powyżej rozwiązaniu.

- **Tożsamość i systemy reputacji:** Gdy zyskasz już możliwość zarejestrowania się w blockchainie, kolejny logiczny krok jest oczywisty — jest nim przeniesienie do tegoż łańcucha sieci zaufania. Sieci zaufania są kluczowym elementem efektywnej infrastruktury komunikacyjnej *peer-to-peer*: nie tylko chcesz wiedzieć, czy dany klucz publiczny odnosi się do danej osoby; zależy Ci również na ustaleniu, czy ta osoba jest w ogóle godna zaufania. Rozwiązaniem jest użycie sieci społecznościowych: jeśli ufasz A, A ufa B, natomiast B ufa C, istnieje spore prawdopodobieństwo, że możesz ufać C — przynajmniej do pewnego stopnia. Ethereum może służyć jako warstwa danych w pełni zdecentralizowanego systemu reputacji, a ostatecznie także w pełni zdecentralizowanego rynku.

Wiele spośród wymienionych powyżej zastosowań odwołuje się do protokołów lub inicjatyw *peer-to-peer*, które są już rozwijane; w tych przypadkach chcielibyśmy nawiązać relacje partnerskie z jak najliczniejszą grupą takich projektów i wspierać je finansowo w zamian za korzyści, jakie mogą one zapewnić ekosystemowi Ethereum. Pragniemy pomagać nie tylko społeczności związanej z kryptowalutami, ale także całej społeczności *peer-to-peer*, do której zaliczają się osoby korzystające z udostępniania plików, torrentów, zdecentralizowanego przechowywania danych i sieci mesh. Jesteśmy przekonani, że nie brakuje projektów — zwłaszcza tych niezwiązanych z kwestiami finansowymi — które mogą potencjalnie zapewniać społeczności mnóstwo korzyści, ale ich rozwój powstrzymywany jest przez niedobór funduszy wynikający z niemożności skutecznego wprowadzenia do tych inicjatyw komponentu finansowego. Niewykluczone, że Ethereum okaże się czynnikiem, który pozwoli dziesiątkom takich projektów przejść do kolejnej fazy rozwoju.

Jak to w ogóle możliwe, że Ethereum zapewnia podstawy dla wszystkich tych zastosowań? Odpowiedzią jest specyfika wewnętrznego języka programowania tej waluty. W tym miejscu mogę przywołać porównanie do internetu: w 1996 r. sieć korzystała wyłącznie z języka HTML, co pozwalało jedynie na tworzenie statycznych witryn w rodzaju GeoCities. Potem deweloperzy uświadomili sobie, że powinni jak najszybciej zapewnić użytkownikom możliwość wypełniania tworzonych w HTML-u formularzy, tak

więc we wspomnianym języku pojawiła się stosowna funkcjonalność. Był to odpowiednik kolorowanych monet w świecie protokołów sieciowych — próba rozwiązania specyficznego problemu, aczkolwiek zrealizowana na fundamentach niedoskonałego protokołu i bez uwzględniania szerszego obrazu sytuacji. Wkrótce pojawił się jednak JavaScript — język programowania działający w przeglądarkach internetowych — i to właśnie on okazał się rozwiązaniem problemu. Ponieważ JavaScript jest uniwersalnym językiem programowania, który posiada cechę kompletności Turinga, może posłużyć do tworzenia aplikacji o dowolnym stopniu złożoności: przy użyciu tego języka napisano Gmaila, Facebooka, a nawet portfele bitcoinowe. Co istotne, do tego wszystkiego nie doszło wcale dlatego, że deweloperzy JavaScriptu uznali, iż chcą, żeby ludzie stworzyli Gmaila, Facebooka i portfele kryptowalutowe; zależało im tylko na udostępnieniu innym języka programowania. O tym, co zdołamy zrobić z takim językiem, decyduje nasza wyobraźnia. Dokładnie takiego ducha chcieliśmy wnieść do projektu Ethereum. Nie zakładamy, że stworzymy coś, co położy kres wszelkim innowacjom w świecie kryptowalut; tak naprawdę Ethereum ma być zaledwie punktem wyjścia.

DALSZY ROZWÓJ

Jeśli nie liczyć głównej funkcjonalności, czyli uniwersalnego języka skryptowego posiadającego cechę kompletności Turinga, Ethereum będzie też w porównaniu do istniejących już kryptowalut krokiem naprzód w wielu innych sferach, do których zaliczają się:

- **Opłaty:** Kontrakty Ethereum będą regulować jego funkcjonalność wynikającą z kompletności Turinga, a opłaty transakcyjne za każdy etap wykonania skryptu będą zapobiegać nadużyciom w rodzaju zajmowania zbyt dużej ilości pamięci i tworzenia nieskończonych pętli. Droższym operacjom, chociażby dostępowi do pamięci masowej czy operacjom kryptograficznym, będą towarzyszyły wyższe opłaty; oprócz tego wprowadzona zostanie też opłata za każdy obiekt przechowywany przez kontrakt. Coś takiego ma zachęcać do tworzenia kontraktów, które będą zostawiać po sobie porządek — jeżeli kontrakt

ograniczy wykorzystywaną przestrzeń dyskową, opłata stanie się wartością ujemną. Tak naprawdę istnieje specjalny kod operacji, SUICIDE, który pozwala usunąć kontrakt, a potem przesyła jego twórcy wszystkie fundusze i sporą premię.

- **Algorytmy kopania:** Pomysł stworzenia kryptowalut, których kopanie byłoby odporne na użycie wyspecjalizowanego sprzętu (co pozwalałoby zaangażować się w te działania zwykłym użytkownikom typowych komputerów, nie zmuszałoby nikogo do jakichkolwiek inwestycji i pomagałoby uniknąć centralizacji), cieszy się sporym zainteresowaniem. Jak na razie głównym antidotum na ten problem był Scrypt — algorytm kopania, który wymaga zarówno sporej mocy obliczeniowej, jak i dużej ilości pamięci. Okazuje się jednak, że wymagania tego algorytmu dotyczące pamięci nie są wystarczająco duże i nie brakuje już firm, które konstruują z myślą o nim wyspecjalizowane urządzenia. W tej sytuacji stworzyliśmy Daggera (czyli prototyp rozwiązania, które odwołuje się do dowodu pracy i ma jeszcze większe wymagania dotyczące pamięci niż Scrypt), a także nowatorskie algorytmy takie jak Slasher, który bazuje na dowodzie stawki i pozwala całkowicie obejść problemy towarzyszące kopaniu. Ostatecznie planujemy jednak zorganizować konkurs przypominający te wydarzenia, które pozwoliły stworzyć standardy AES i SHA3 — zaprosimy do udziału grupy badawcze z uniwersytetów z całego świata, a potem poprosimy tych specjalistów o opracowanie takiego algorytmu kopania, który będzie maksymalnie przyjazny dla posiadaczy zwykłych komputerów.
- **GHOST:** GHOST jest nowym protokołem propagacji bloków stworzonym przez Aviva Zohara i Yonatana Sompolinsky'ego. To rozwiązanie zdecydowanie skraca w blockchainach czas potwierdzenia bloku (w idealnej sytuacji mieści się on w przedziale 3 – 30 sekund), a zarazem nie nastręcza problemów związanych z centralizacją i dużą liczbą osieroconych bloków, czyli kłopotów pojawiających się zwykle w ślad za skróconym czasem potwierdzenia bloku. Ethereum jest pierwszym dużym systemem walutowym, który włączy do swojego protokołu uproszczoną, jednopoziomową wersję GHOST-a.

PLAN

Ethereum może się okazać bardzo rozbudowanym przedsięwzięciem i niewykluczone, że prace rozwojowe dotyczące tej inicjatywy pochłoną wiele miesięcy. Mając na względzie tę kwestię, postanowiliśmy podzielić proces uruchamiania tego projektu na wiele etapów. Pierwszą fazę, czyli publikację białej księgi, mamy już za sobą. Uruchomiliśmy też fora internetowe, wiki i bloga — każdy zainteresowany może je odwiedzić, założyć tam konto i zacząć publikować komentarze na forach. 25 stycznia podczas konferencji w Miami zacznie się 60-dniowy okres zbierania funduszy. W tym czasie każdy będzie mógł kupić za bitcoiny eter, czyli wewnętrzną walutę Ethereum, a cały ten proces będzie bardzo przypominał zbiórkę funduszy zrealizowaną przy okazji powstania mastercoina. Ustalona przez nas cena to 1000 ETH za 1 BTC, aczkolwiek osoby, które zaangażują się w ten projekt na wczesnym etapie, będą mogły liczyć na dwukrotnie większe korzyści, co ma zrekompensować większe ryzyko, jakie podejmują, dołączając wcześniej do całego projektu. Osoby, które przyłączą się do tej zbiórki, otrzymają nie tylko jednostki eteru — mogą też liczyć na dodatkowe nagrody w rodzaju darmowych biletów na konferencje czy możliwości umieszczenia 32 bitów danych w pierwszym bloku łańcucha. Najwięksi donatorzy będą nawet mogli nazwać trzy podjednostki waluty (a więc odpowiedniki mikroBTC w świecie bitcoina).

Emisja eteru nie będzie się ograniczała do wykorzystania jednego mechanizmu — zamiast tego planujemy czerpać korzyści z wielu różnych rozwiązań. Model emisji będzie wyglądał następująco:

Jednostki eteru będą sprzedawane w ramach akcji gromadzenia środków; cena będzie wynosiła od 1000 do 2000 ETH za BTC, a osoby, które dołączą do inicjatywy wcześniej, będą miały zapewnione lepsze warunki, co ma związek z większym ryzykiem towarzyszącym zaangażowaniu się w projekt na wcześniejszym etapie. Minimalna wpłata ma wynosić 0,01 BTC. Przyjmijmy, że cała ta akcja doprowadzi do wyemitowania *x* jednostek ETH:

- 0,225 z *x* jednostek ETH zostanie przekazane powiernikom i osobom, które miały znaczący wkład w ten projekt jeszcze przed rozpoczęciem zbiórki funduszy. Ta część jednostek będzie przez pewien czas zablokowana: po upływie roku będzie można wydać około 40 procent tych środków, po dwóch latach — 70 procent, a po trzech latach — 100 procent.

- 0,05 z *x* jednostek ETH posłuży do stworzenia funduszu wykorzystywanego do finansowania wydatków i nagród wypłacanych w jednostkach eteru między rozpoczęciem zbiórki środków a wprowadzeniem waluty do obrotu.
- 0,225 z *x* jednostek ETH posłuży do stworzenia długoterminowej rezerwy, która umożliwi sfinansowanie wydatków, pensji i wypłacanych w jednostkach eteru nagród po wprowadzeniu waluty do obrotu.
- 0,4 z *x* jednostek ETH to pula, która od tego momentu będzie co roku wykopywana przez górników.

W porównaniu z bitcoinem i większością innych kryptowalut widać tutaj znaczącą różnicę: podaż jest zasadniczo nieograniczona. Model „stałej liniowej inflacji" został skonstruowany w taki sposób, żeby eter mógł uniknąć zarówno spadku, jak i wzrostu siły nabywczej; brak ograniczenia podaży ma zredukować problemy spekulacji i nierównomiernej dystrybucji majątku towarzyszące istniejącym już walutom, choć użycie liniowego modelu inflacji (zamiast popularniejszego modelu wykładniczego) oznacza również, że realna inflacja będzie zmierzać z czasem do zera. Co więcej, ponieważ początkowa podaż waluty będzie większa od zera, wzrost podaży waluty przez pierwszych osiem lat będzie tak naprawdę niższy, niż miało to miejsce w przypadku bitcoina, dzięki czemu uczestnicy początkowej zbiórki i użytkownicy, którzy zdecydują się dołączyć do projektu na wczesnym etapie jego rozwoju, będą mogli liczyć w perspektywie średnioterminowej na znaczące korzyści.

W którymś momencie w lutym uruchomimy scentralizowany testnet — serwer umożliwiający wszystkim użytkownikom realizowanie transakcji i tworzenie kontraktów. Niewiele później powstanie zdecentralizowany testnet, który pozwoli nam sprawdzić różne algorytmy kopania i upewnić się, że demon *peer-to-peer* funkcjonuje tak, jak należy, i jest odpowiednio zabezpieczony. Przy okazji przeprowadzimy też pomiary, dzięki którym będziemy mogli zoptymalizować język skryptowy. Gdy już potwierdzimy solidność protokołu i klienta, udostępnimy pierwszy blok i umożliwimy rozpoczęcie kopania.

WYGLĄDAJĄC W PRZYSZŁOŚĆ

Ponieważ Ethereum skrywa w sobie język skryptowy posiadający cechę kompletności Turinga, można matematycznie dowieść, że nie ustępuje pod względem możliwości przypominającej bitcoina kryptowalucie bazującej na łańcuchu bloków. Ten protokół wciąż skrywa jednak kilka problemów, które jak na razie pozostają nierozwiązane. Ethereum nie zapewnia na przykład rozwiązania zasadniczego problemu skalowalności trapiącego wszystkie kryptowaluty bazujące na blockchainie — chodzi o to, że każdy pełny węzeł powinien przechowywać kompletny bilans waluty i musi weryfikować wszystkie transakcje. Zapożyczona z Ripple koncepcja oddzielenia od siebie „drzewa stanu" i „listy transakcji" pozwala do pewnego stopnia ograniczyć dokuczliwość tego problemu, ale nie udało mi się dokonać w tej kwestii żadnego przełomu. Żeby był on możliwy, musimy zaczekać na dokończenie prac nad rozwiązaniem takim jak Secure Computational Integrity and Privacy (SCIP) Eliego Ben-Sassona.

Oprócz tego Ethereum nie zapewnia żadnych postępów w stosunku do tradycyjnego kopania i modelu dowodu pracy (wraz z wszystkimi ich wadami), a kwestia dowodu doskonałości i model konsensusu wykorzystywany przez Ripple nie zostały na razie dokładniej zbadane. Gdyby okazało się, że dowód stawki lub jakiś inny algorytm dowodu pracy jest lepszym rozwiązaniem, przyszłe kryptowaluty mogłyby wykorzystywać algorytmy dowodu stawki takie jakie MC2 i Slasher. Jeśli pojawi się przestrzeń pozwalająca stworzyć Ethereum 2.0, wprowadzane udoskonalenia będą dotyczyły właśnie wymienionych powyżej kwestii. Ostatecznie Ethereum jest otwartym projektem — jeżeli zgromadzimy wystarczająco duże fundusze, niewykluczone, że sami stworzymy Ethereum 2.0, przenosząc założone wcześniej konta do nowej, jeszcze doskonalszej sieci. Zgodnie z tym, co głosi slogan dotyczący naszej waluty, jedynym ograniczeniem jest nasza wyobraźnia.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

Ta książka jest (...) próbą ustalenia, w jaki sposób można zmieniać świat na lepsze.

Jaron Lanier, informatyk i autor

łańcuch bloków ma wyjątkowy potencjał. W najśmielszym scenariuszu może doprowadzić do odebrania władzy politykom i wielkim firmom, aby rozdzielić ją między użytkowników. Chodzi tu o odniesienie nie tylko do kryptowalut, ale także organizacji i społeczności. Dziś sieć Ethereum zapewnia podstawy techniczne walucie ether, tokenom NFT i zdecentralizowanym autonomicznym organizacjom. Nie wiemy jednak, jak będzie wyglądać przyszłość Ethereum. Może się stać utopią, dystopią i wszystkim, co mieści się między tymi skrajnościami.

Ta książka jest unikalnym zbiorem esejów napisanych przez twórcę sieci Ethereum. W swoim czasie stanowiły one zbiór wskazówek dla społeczności Ethereum, dziś ich znaczenie może być o wiele większe. Buterin, jako kreatywny myśliciel, z odwagą zgłębia możliwe kierunki rozwoju swojego wynalazku i prezentuje łańcuch bloków jako szeroką gamę możliwości społecznych, ekonomicznych i politycznych. Lektura tej książki wymaga odwagi, gdyż niektóre ze wspomnianych scenariuszy rozwoju mogą prowadzić do przerażających konsekwencji. Tym bardziej jednak jest to niezwykle ważna pozycja — w tej chwili niemal wszystkie opcje ewolucji Ethereum pozostają otwarte i dlatego potrzebna jest szeroka dyskusja o przyszłości technologii stanowiącej fundament tej sieci.

Vitalik Buterin jest rosyjsko-kanadyjskim programistą i pisarzem. W 2011 roku współzakładał „Bitcoin Magazine", a w 2014 doprowadził do powstania sieci Ethereum. W 2021 roku „Time" przyznał mu tytuł jednego z najbardziej wpływowych ludzi na świecie.

Helion onepress

Księgarnia internetowa:
http://onepress.pl

HELION SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
onepress@onepress.pl

książkiklasybusiness

ebook dostępny na:
ebookpoint

ISBN 978-83-289-0201-5

9 788328 902015

Cena: 67,00 zł

SEVEN STORIES