CZY KUPIĆ BITCOINA?

1. Liczba bitcoinów jest sztywno ograniczona.

Liczba bitcoinów, która kiedykolwiek zostanie stworzona, jest stała i sztywno ograniczona. Liczby tej nigdy nie będzie można zwiększyć. Ta ograniczona podaż jest główną zaletą bitcoina i źródłem jego wartości.

Bitcoin (skrót: BTC) został stworzony przez anonimowego twórcę o pseudonimie Satoshi Nakamoto w odpowiedzi na kryzys finansowy z lat 2007-2008, spowodowany nadmierną podażą pieniądza i nieuczciwą inżynierią finansową. Aby zapobiec tego rodzaju kryzysom, oraz inflacji prowadzącej do utraty wartości pieniądza, należało stworzyć pieniądz o ściśle określonej, niezmiennej, stałej i pewnej podaży. Liczba bitcoinów została sztywno określona (na 21 milionów sztuk) w algorytmie (oprogramowaniu) określającym funkcjonowanie sieci bitcoina.

Nowe bitcoiny są wytwarzane co około 10 minut (jako nagroda dla "górników" za pomyśle zatwierdzenie kolejnego wpisu w rejestrze – zwanego blokiem), ale liczba nowopowstających bitcoinów zmniejsza się co 4 lata w procesie znanym "halvingiem". Na początku co 10 minut powstawało 50 bitcoinów, obecnie powstaje 6.25 BTC. W kwietniu lub w maju 2024 r. nastąpi następny "halving" i co dziesięć minut powstawać będzie nieco ponad 3 bitcoiny (3.125). Następne „halvingi” nastąpią w 2028, 2032, 2036 itd. Do roku 2034 wyemitowanych zostanie 99% wszystkich "monet". Przykładowo w roku 2060 co 10 minut powstawać będzie już tylko 0,006 BTC. Ostatnie monety zostaną wyemitowane około 2140 roku. Dokładna rozpiska przyszłych „halvingów” i wielkości emisji znajduje się tutaj: https://www.pnbitcoin.com/pnbitcoin/block-reword.

Podaż ta jest sztywno określona i niezmienna. Nigdy nie będzie można jej zmienić. Nigdy nie zostanie wyemitowanych więcej bitcoinów, niż zostało to zaprogramowane. Ani za 10 lat, ani za 100, ani za 1000. Żadna osoba ani instytucja nie będzie mogła "dodrukować" dodatkowych bitcoinów lub zwiększyć ich ilości w systemie informatycznym (co się zdarza na porządku dziennym z klasycznymi pieniędzmi).

2. Liczba bitcoinów jest niewielka.

Liczba bitcoinów jest nie tylko ograniczona, ale także stosunkowo niewielka. Ostateczna ilość to 21 milionów (zostanie osiągnięta w roku 2140), z czego już obecnie w obiegu jest ponad 19 i pół miliona (dokładną liczbę można znaleźć tutaj: https://blockchain.info/q/totalbc). Szacuje się, że około 20-30% bitcoinów zostało na zawsze utraconych (ich właściciele utracili do nich dostęp).

Przez kolejne ponad 100 lat zostanie wyprodukowanych nie więcej niż około półtora miliona bitcoinów. Jak wcześniej wspomniano, liczba ta nie może ulec zwiększeniu. Tak więc podaż nowych monet (inflacja) jest stała i ulega systematycznemu zmniejszeniu (ostatecznie do zera). Nawet przy stałym popycie oznacza to wzrost ceny. Tymczasem popyt, przynajmniej dotychczas, systematycznie rośnie. Rosnący popyt i malejąca podaż będzie mieć oczywisty wpływ na cenę.

3. Bitcoin jest zdecentralizowany.

Aby stworzyć pieniądz o stałej podaży, konieczne było wyeliminowanie "centralnej instytucji" odpowiedzialnej za emisję pieniądza. Inaczej podaż nie byłaby naprawdę stała. Nawet jeśli "centralna instytucja" zobowiązałaby się ograniczyć podaż, to byłoby to jedynie zobowiązanie, którego można by nie dotrzymać (co wielokrotnie miało miejsce w przypadku podmiotów emitujących tradycyjne pieniądze). Dokładnie tego chciał uniknąć Satoshi Nakamoto.

Konieczne było więc stworzenie waluty, która nie byłaby emitowana przez "centralną instytucję" (bank, państwo), czyli walutę zdecentralizowaną.

Jednakże w przypadku walut zdecentralizowanych (próby ich stworzenia były podjęte wcześniej) pojawił się problem "podwójnego wydatkowania" (*double spending*). W przypadku waluty zdecentralizowanej brak jest centralnego rejestru, w którym przechowywane byłyby wartości poszczególnych kont i w którym zapisywane byłyby transakcje. W przypadku tradycyjnego pieniądze dane te zapisywane są w centralnym rejestrze prowadzonym np. przez bank. Jeśli klient banku chce wykonać przelew, centrala potwierdza, że klient A ma te środki, a następnie przekazuje je do klienta B, zmieniając wpisy w rejestrze centralnym.

Jeśli nie ma centralnej instytucji, nie ma centralnego rejestru sald (kto ile ma) i transakcji (co kto komu wysłał). Brak takiego rejestru powoduje problemy z weryfikacją sald i transakcji, w tym problem "podwójnego wydawania" (*double spending*).

Twórca bitcoina rozwiązał ten problem dzięki **tzw. rozproszonemu rejestrowi** (*distributed ledger*) i technologii blockchain. W skrócie, rejestr sald kont i transakcji nie jest prowadzony przez jedną centralną instytucję (bank, państwo), ale przez wiele podmiotów, które uruchomiły odpowiednie oprogramowanie i podłączyły się do sieci. Gdy klient A chce przelać bitcoina do klienta B, wysyła zapytanie do odpowiedniej liczby podmiotów prowadzących ten rejestr. Jeśli wystarczająca liczba podmiotów potwierdzi, że klient A ma bitcoina, dochodzi do "przeniesienia" środków, zmieniając wpisy w rejestrach klienta A i B. Tworzy się nowa transakcja w blockchainie, zmieniając saldo dwóch podmiotów, a ta nowa informacja o saldach i transakcjach jest wysyłana do wszystkich podmiotów prowadzących rejestr bitcoina.

Tak więc podmioty prowadzące rejestr bitcoina dokonują weryfikacji transakcji, przechowując dane o saldach kont i o historii transakcji.

Dlaczego to robią?

Twórca bitcoina przewidział dla nich wynagrodzenie. Jak wyżej wspomniano co około 10 minut algorytm bitcoina tworzy określoną liczbę nowych monet, które są rozdzielane pomiędzy podmioty prowadzące rejestr bitcoina (konkretnie do górnika, który dokonał walidacji bloku). Te nagrody stanowią motywację (bodziec) do utrzymywania oprogramowania obsługującego sieć bitcoina i rozproszony rejestr. Celem osób utrzymujących zdecentralizowany rejestr bitcoina (tzw. górników) jest uzyskanie (wydobycie) nowych monet. Skutkiem jest natomiast zabezpieczenie i utrzymywanie sieci bitcoina.

Jednocześnie wprowadzono mechanizmy, które faworyzują najpotężniejsze komputery (górnik dysponujący mocniejszym komputerem ma większe szanse na weryfikację bloku, a tym samym na wydobycie nowych monet). To prowadzi do rodzaju "wyścigu zbrojeń", a w rezultacie sieć bitcoina staje się coraz mocniejsza. Obecnie sieć bitcoina jest obsługiwana przez miliony komputerów o łącznej mocy obliczeniowej kilkuset tysięcy razy większej niż najlepszy superkomputer.

4. Bezpieczeństwo - sieci, portfela i transakcji

Bezpieczeństwo bitcoina ma charakter wielopłaszczyznowy.

Po pierwsze, jest to **bezpieczeństwo sieci**. Jak już wspomniano, sieć bitcoina jest najpotężniejszą siecią komputerową na świecie (stale rosnącą w siłę).

Ogromna moc obliczeniowa zabezpiecza sieć. Im więcej komputerów uczestniczmy w sieci, im więcej mocy obliczeniowej jest zużywanej na "wykopywanie" bitcoina (a co za tym idzie im więcej energii jest zużywanej), tym sieć bitcoina jest silniejsza i bardziej odporna na ataki (obecnie tzw. atak 51% jest w zasadzie niemożliwy, a na pewno niecelowy). Sieć bitcoina nigdy nie została zhakowana (zhakowane zostały giełdy centralne handlujące bitcoinem). Oprogramowanie bitcoina jest otwarte i jawne (*open-source*) i zostało wielokrotnie przeanalizowane przez niezliczonych ekspertów ds. bezpieczeństwa i informatyków. Ponadto "górnicy", którzy utrzymują sieć, są rozmieszczeni na całym świecie, co oznacza, że nie ma pojedynczych punktów awarii lub ataku.

Po drugie, jest to **bezpieczeństwo portfela użytkowników.**
Gdy założysz konto w sieci bitcoina, dostęp do niego będzie chroniony przez „klucz prywatny", tj. przez ciąg 64 cyfr i znaków, lub przez tzw. frazę *seed*, tj. przez 12 losowo wybranych słów w języku angielskim.

Z uwagi na ilość kombinacji (340,282,366,920,938,463,463,374,607,431,768,211,456) nie ma możliwości zgadnięcia / przełamania / zhakowania ww. zabezpieczania.

Powyższy klucz prywatny lub kombinacja 12 słów stanowią 100% pewne, ale i jedynie zabezpieczanie ww. portfela. Oznacza to z jednej strony, iż dysponując wyłącznie ww. danymi możesz w każdym czasie i miejscu uzyskać dostęp do ww. środków (i nimi rozdysponować). Nie ma potrzeby ani możliwości jakiegokolwiek dodatkowego potwierdzenia transakcji. Tak więc wszystkie dane potrzebne do dostępu do bitcoina można zapisać na karteczce lub zapamiętać.

Z drugiej strony każda osoba dysponujące ww. danymi może uzyskać dostęp do portfela BTC, dlatego też tak ważna jest ich ochrona. Dane te należy chronić przed innymi osobami, ale również przed zgubieniem (w takim przypadku nie ma żadnej możliwości ich odzyskania, a dostęp do bitcoinów zostaje utracony na zawsze).
Po trzecie jest to **bezpieczeństwo wynikające z zdecentralizowania** i braku konieczności zaufania komukolwiek. bitcoin działa w sieci zdepenalizowanej, bez centralnego organu zarządzającego, bez

CEO, bez pośredników, bez zarządu itd. Wszelkie dane dotyczące każdego portfela są zapisane bezpośrednio w rozproszonym rejestrze bitcoina, a więc na milionach komputerów. Integralność tych danych chroni najmocniejsza sieć na świecie. Oznacza to, iż w odróżnieniu od banków, brokerów, giełd i innych pośredników, sieć bitcoina nie może upaść, uciec lub oszukać. Nie ma żadnych osób, którym należałoby zaufać. Wszystko opiera się na algorytmie komputerowym, a nie na zaufaniu do ludzi.

Oznacza to również **bezpieczeństwo transakcji.** Pozytywnie zweryfikowana transakcja jest ostateczna. Nie można jej anulować ani cofnąć. Nikt nie może prawidłowej transakcji zamrozić, zatrzymać lub zablokować (nikt, w tym również organy ścigania, sądy, banki itd.). Jeżeli transakcja spełnia wymagania sieci (przede wszystkim nadawca posiada środki, które wysyła), to zostanie ona zrealizowana i będzie nieodwracalna.

5. Jak zacząć?

Bitcona (i inne kruptowaluty) najłatwiej i najbezpieczniej nabyć na jednej z "scentralizowanych giełd", będących rodzajem pośrednika. Spis tutaj: https://www.satoshingmx.com/cex
Największą giełdą jest Binance. Płacić można kartą lub przelewem.

Po zakupie bitcoina powinno się przelać na "portfel zewnętrzny", tj. portfel założony bezpośrednio w blockchainie. Dopiero wówczas tak na prawdę posiada się bitcoina, ma się dostęp do portfela chronionego przez 12 słów i korzysta się w pełni z zalet bitcoina opisanych powyżej. Przykład takiego portfela jest tutaj: www.trustwallet.com. Inne portfele możesz znaleźć tutaj: https://bitcoin.org/en/choose-your-wallet

Kiedy kupić bitcoina? Jeżeli traktujesz BTC jako długoterminową inwestycję i nie zamierzasz nim handlować lub spekulować, to zastosowanie znajduje klasyk: "najlepszy moment na zakup bitcoina był 10 lat temu, drugi najlepszy jest teraz".

Wszystko co wyżej napisałem nie jest poradą inwestycyjną ani finansową. Cokolwiek zrobisz, robisz to na własne ryzyko.
Natomiast prawda jest taka, iż nikt kto dotychczas kupił bitcoina i trzymał go na zewnętrznym portfelu przez co najmniej 2-3 lata (nie gubiąc 12 słów), na transakcji tej nie stracił. NIKT, NIGDY!

Kontakt do mnie: czykupicbitcona@gmail.com.