Jak działają kryptowaluty?

Grzegorz Kosiorowski

Uniwersytet Ekonomiczny w Krakowie

Kryptowaluta? O co chodzi? Nieporozumienia.

Kryptowaluta? O co chodzi? Nieporozumienia.

- Powszechne rozumienie: „wirtualne pieniądze” oparte o algorytm kryptograficzny, najczęściej znajdujące się poza kontrolą zewnętrznych organizacji np. państw.

Kryptowaluta? O co chodzi? Nieporozumienia.

- Powszechne rozumienie: „wirtualne pieniądze” oparte o algorytm kryptograficzny, najczęściej znajdujące się poza kontrolą zewnętrznych organizacji np. państw.
- Krypto? Tak. Waluta? Nie do końca.

Kryptowaluta? O co chodzi? Nieporozumienia.

- Powszechne rozumienie: „wirtualne pieniądze” oparte o algorytm kryptograficzny, najczęściej znajdujące się poza kontrolą zewnętrznych organizacji np. państw.
- Krypto? Tak. Waluta? Nie do końca.
- Czy kryptowaluty to coś „fizycznego”? Portfele? Wykopywanie kryptowalut? Kopacze/górnicy?

Kryptowaluta? O co chodzi? Nieporozumienia.

- Powszechne rozumienie: „wirtualne pieniądze” oparte o algorytm kryptograficzny, najczęściej znajdujące się poza kontrolą zewnętrznych organizacji np. państw.
- Krypto? Tak. Waluta? Nie do końca.
- Czy kryptowaluty to coś „fizycznego”? Portfele? Wykopywanie kryptowalut? Kopacze/górnicy?
- Czy kryptowaluty łamią zasady ekonomii? Dowód pracy? Wartość oparta na pracy?

Kryptowaluta - tak naprawdę

Kryptowaluta - tak naprawdę

- Kryptowaluta: dziennik transakcji (system księgowania).

Kryptowaluta - tak naprawdę

- Kryptowaluta: dziennik transakcji (system księgowania).
- Rejestruje transakcje użytkowników sieci kontaktów.

Kryptowaluta - tak naprawdę

- Kryptowaluta: dziennik transakcji (system księgowania).
- Rejestruje transakcje użytkowników sieci kontaktów.
- Dostęp do indywidualnych zasobów kryptograficznie zabezpieczony dla posiadacza prywatnego kodu.

Kryptowaluta - tak naprawdę

- Kryptowaluta: dziennik transakcji (system księgowania).
- Rejestruje transakcje użytkowników sieci kontaktów.
- Dostęp do indywidualnych zasobów kryptograficznie zabezpieczony dla posiadacza prywatnego kodu.
- System rozproszony: nie wymaga organu nadzorującego ani zaufania między użytkownikami.

Kryptowaluta - tak naprawdę

- Kryptowaluta: dziennik transakcji (system księgowania).
- Rejestruje transakcje użytkowników sieci kontaktów.
- Dostęp do indywidualnych zasobów kryptograficznie zabezpieczony dla posiadacza prywatnego kodu.
- System rozproszony: nie wymaga organu nadzorującego ani zaufania między użytkownikami.
- Każdy może taki system stworzyć (choć efektywnie wymaga zaangażowania dużej liczby użytkowników).

Odrobina historii

Odrobina historii

- 2009 rok: Ogólnodostępny artykuł „Bitcoin: A Peer-to-Peer Electronic Cash System" Satoshiego Nakamoto (pseudonim): technologia blockchain.

Odrobina historii

- 2009 rok: Ogólnodostępny artykuł „Bitcoin: A Peer-to-Peer Electronic Cash System" Satoshiego Nakamoto (pseudonim): technologia blockchain.
- Pierwsza i najbardziej znana kryptowaluta: Bitcoin.

Odrobina historii

- 2009 rok: Ogólnodostępny artykuł „Bitcoin: A Peer-to-Peer Electronic Cash System" Satoshiego Nakamoto (pseudonim): technologia blockchain.
- Pierwsza i najbardziej znana kryptowaluta: Bitcoin.
- Później powstały: Ethereum, Tether, Litecoin, Ripple i wiele innych.

O czym będzie, a o czym nie

O czym będzie, a o czym nie

- Temat: jak to działa? Jakie prawa matematyki stoją za powstaniem kryptowalut?

O czym będzie, a o czym nie

- Temat: jak to działa? Jakie prawa matematyki stoją za powstaniem kryptowalut?
- Nie: jak inwestować w kryptowaluty? Czy warto? Czy to bezpieczne?

O czym będzie, a o czym nie

- Temat: jak to działa? Jakie prawa matematyki stoją za powstaniem kryptowalut?
- Nie: jak inwestować w kryptowaluty? Czy warto? Czy to bezpieczne?
- Nie: czy kryptowaluty to przyszłość?

Kryptologia na ratunek

Na moim jesiennym wykładzie przedstawiłem osiągnięcia kryptologii, które pozwalają na istnienie kryptosystemów z kluczem publicznym.

Kryptosystem z kluczem publicznym

Istnieją algorytmy, według których wiadomości łatwo i szybko szyfrowane za pomocą klucza publicznego (jawnego dla wszystkich zainteresowanych) mogą być w rozsądnym czasie rozszyfrowane tylko przez osobą znającą klucz prywatny (tajny).

Dziennik rozliczeń

Dziennik rozliczeń

- Aurora, Beatrycze, Cieszygor i Dzierżykraj przeprowadzają wspólnie dużo transakcji (np. wspólnie mieszkają i na przemian robią zakupy, zamawiają jedzenie, opłacają media i czynsze). Nie opłaca się im rozliczać po każdym takim wydarzeniu, tylko np. co miesiąc.

Dziennik rozliczeń

- Aurora, Beatrycze, Cieszygor i Dzierżykraj przeprowadzają wspólnie dużo transakcji (np. wspólnie mieszkają i na przemian robią zakupy, zamawiają jedzenie, opłacają media i czynsze). Nie opłaca się im rozliczać po każdym takim wydarzeniu, tylko np. co miesiąc.
- Po każdej transakcji zapisują, w „dzienniku rozliczeń" kto ile pieniędzy powinien otrzymać w rozliczeniu i od kogo (np. Aurora otrzyma 15 złotych od Dzierżykraja, po tym jak zapłaciła za pizzę, którą wspólnie zjedli).

Dziennik rozliczeń

- Aurora, Beatrycze, Cieszygor i Dzierżykraj przeprowadzają wspólnie dużo transakcji (np. wspólnie mieszkają i na przemian robią zakupy, zamawiają jedzenie, opłacają media i czynsze). Nie opłaca się im rozliczać po każdym takim wydarzeniu, tylko np. co miesiąc.
- Po każdej transakcji zapisują, w „dzienniku rozliczeń" kto ile pieniędzy powinien otrzymać w rozliczeniu i od kogo (np. Aurora otrzyma 15 złotych od Dzierżykraja, po tym jak zapłaciła za pizzę, którą wspólnie zjedli).
- Na koniec miesiąca osoby, które są "winne" więcej niż mają otrzymać, wpłacają różnicę do wspólnej puli, by osoby, które powinny otrzymać zwrot, mogły z tej puli wypłacić.

Dziennik rozliczeń: przykład

Kto otrzyma	Kto zapłaci	Ile
Aurora	Dzierżykraj	15
Beatrycze	Aurora	10
Cieszygor	Beatrycze	50
Dzierżykraj	Beatrycze	5

Dziennik rozliczeń: przykład

Kto otrzyma	Kto zapłaci	Ile
Aurora	Dzierżykraj	15
Beatrycze	Aurora	10
Cieszygor	Beatrycze	50
Dzierżykraj	Beatrycze	5

Na koniec miesiąca Beatrycze wpłaci do puli 45, Dzierżykraj 10, Aurora pobierze 5, a Cieszygor 50.

Dziennik rozliczeń: przykład

Kto otrzyma	Kto zapłaci	Ile
Aurora	Dzierżykraj	15
Beatrycze	Aurora	10
Cieszygor	Beatrycze	50
Dzierżykraj	Beatrycze	5

Na koniec miesiąca Beatrycze wpłaci do puli 45, Dzierżykraj 10, Aurora pobierze 5, a Cieszygor 50.

Jak powstrzymać fałszywe wpisy?

Podpisy cyfrowe

Każda transakcja musi być podpisana przez „dłużnika”! Zatem dziennik wygląda tak:

Kto otrzyma	Kto zapłaci	Ile	Podpis
Aurora	Dzierżykraj	15	Dzierżykraj
Beatrycze	Aurora	10	Aurora
Cieszygor	Beatrycze	50	Beatrycze
Dzierżykraj	Beatrycze	5	Beatrycze

Podpisy cyfrowe

Każda transakcja musi być podpisana przez „dłużnika”! Zatem dziennik wygląda tak:

Kto otrzyma	Kto zapłaci	Ile	Podpis
Aurora	Dzierżykraj	15	Dzierżykraj
Beatrycze	Aurora	10	Aurora
Cieszygor	Beatrycze	50	Beatrycze
Dzierżykraj	Beatrycze	5	Beatrycze

Ale czy podpisu nie można po prostu skopiować?

Podpisy cyfrowe

Podpis tej samej osoby, przypisany do innej transakcji jest zupełnie inny!

Podpisy cyfrowe

Podpis tej samej osoby, przypisany do innej transakcji jest zupełnie inny!

- Podpis użytkownika to tak naprawdę dwa ciągi liczb: kod publiczny oraz kod prywatny.

Podpisy cyfrowe

Podpis tej samej osoby, przypisany do innej transakcji jest zupełnie inny!

- Podpis użytkownika to tak naprawdę dwa ciągi liczb: kod publiczny oraz kod prywatny.
- Funkcja *Sign* (funkcja znaku) każdej parze: wiadomość wpisana do dziennika i kod prywatny użytkownika przypisuje ciąg (na przykład) 256 znaków: zer i jedynek (bitów), który staje się podpisem cyfrowym. Nawet minimalna zmiana wiadomości powoduje znaczącą zmianę wyniku.

Podpisy cyfrowe

Podpis tej samej osoby, przypisany do innej transakcji jest zupełnie inny!

- Podpis użytkownika to tak naprawdę dwa ciągi liczb: kod publiczny oraz kod prywatny.
- Funkcja *Sign* (funkcja znaku) każdej parze: wiadomość wpisana do dziennika i kod prywatny użytkownika przypisuje ciąg (na przykład) 256 znaków: zer i jedynek (bitów), który staje się podpisem cyfrowym. Nawet minimalna zmiana wiadomości powoduje znaczącą zmianę wyniku.
- Funkcja weryfikująca *Verify* na podstawie wiadomości, podpisu i klucza publicznego szybko sprawdza, czy podpis jest prawidłowy.

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.
Potencjalne problemy:

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.
Potencjalne problemy:

- Obie funkcje powinny być dość szybkie do zastosowania.

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.
Potencjalne problemy:

- Obie funkcje powinny być dość szybkie do zastosowania.
- Odwrócenie funkcji "Sign", czyli znalezienie kodu prywatnego tylko na podstawie kodu publicznego, wiadomości i podpisu powinno być praktycznie niemożliwe.

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.
Potencjalne problemy:

- Obie funkcje powinny być dość szybkie do zastosowania.
- Odwrócenie funkcji "Sign", czyli znalezienie kodu prywatnego tylko na podstawie kodu publicznego, wiadomości i podpisu powinno być praktycznie niemożliwe.
- Kryptosystem z kluczem publicznym!

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.
Potencjalne problemy:

- Obie funkcje powinny być dość szybkie do zastosowania.
- Odwrócenie funkcji "Sign", czyli znalezienie kodu prywatnego tylko na podstawie kodu publicznego, wiadomości i podpisu powinno być praktycznie niemożliwe.
- Kryptosystem z kluczem publicznym!
- W praktyce, by podrobić podpis, nie ma szybszego sposobu niż sprawdzenie wszystkich 2^{256} możliwości.

Dygresja: łamanie podpisu brutalną siłą

Przecież komputery sobie radzą z wielkimi liczbami. Po jakimś czasie, powinien sobie poradzić z 2^{256} możliwości, prawda?

Dygresja: łamanie podpisu brutalną siłą

Przecież komputery sobie radzą z wielkimi liczbami. Po jakimś czasie, powinien sobie poradzić z 2^{256} możliwości, prawda?

- Nie do końca. $2^{256} = (2^{32})^8$, a 2^{32} to nieco ponad 4 miliardy.

Dygresja: łamanie podpisu brutalną siłą

Przecież komputery sobie radzą z wielkimi liczbami. Po jakimś czasie, powinien sobie poradzić z 2^{256} możliwości, prawda?

- Nie do końca. $2^{256} = (2^{32})^8$, a 2^{32} to nieco ponad 4 miliardy.
- Nawet najlepszy superkomputer ma problem z wykonaniem 4 miliardów takich operacji sprawdzania na sekundę.

Dygresja: łamanie podpisu brutalną siłą

Dygresja: łamanie podpisu brutalną siłą

- 4 miliardy galaktyk;

Dygresja: łamanie podpisu brutalną siłą

- 4 miliardy galaktyk;
- W każdej z nich 4 miliardy planet typu Ziemia;

Dygresja: łamanie podpisu brutalną siłą

- 4 miliardy galaktyk;
- W każdej z nich 4 miliardy planet typu Ziemia;
- Na każdej z nich 4 miliardy mieszkańców (ponad połowa) ma do dyspozycji po 4 miliardy takich superkomputerów;

Dygresja: łamanie podpisu brutalną siłą

- 4 miliardy galaktyk;
- W każdej z nich 4 miliardy planet typu Ziemia;
- Na każdej z nich 4 miliardy mieszkańców (ponad połowa) ma do dyspozycji po 4 miliardy takich superkomputerów;
- Pracują przez 4 miliardy razy 4 miliardy sekund = 507 miliardów lat (37 razy wiek wszechświata);

Dygresja: łamanie podpisu brutalną siłą

- 4 miliardy galaktyk;
- W każdej z nich 4 miliardy planet typu Ziemia;
- Na każdej z nich 4 miliardy mieszkańców (ponad połowa) ma do dyspozycji po 4 miliardy takich superkomputerów;
- Pracują przez 4 miliardy razy 4 miliardy sekund = 507 miliardów lat (37 razy wiek wszechświata);
- Szansa, że złamią w tym czasie brutalną siłą kod 256-bitowy to:

Dygresja: łamanie podpisu brutalną siłą

- 4 miliardy galaktyk;
- W każdej z nich 4 miliardy planet typu Ziemia;
- Na każdej z nich 4 miliardy mieszkańców (ponad połowa) ma do dyspozycji po 4 miliardy takich superkomputerów;
- Pracują przez 4 miliardy razy 4 miliardy sekund = 507 miliardów lat (37 razy wiek wszechświata);
- Szansa, że złamią w tym czasie brutalną siłą kod 256-bitowy to:
- 1 do 4 miliardów.

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.

- Podpis zweryfikowany jako prawdziwy oznacza w praktyce, że transakcja jest prawdziwa.

Podpisy cyfrowe

Sign(wiadomość,kod prywatny)= podpis
Verify(wiadomość, podpis, kod publiczny)= prawda/fałsz.

- Podpis zweryfikowany jako prawdziwy oznacza w praktyce, że transakcja jest prawdziwa.
- A co jeśli ktoś skopiowałby do systemu całą transakcję, wraz z podpisem?

Dziennik transakcji

Wystarczy na początku do wiadomości opisującej transakcję dodać jej numer. W ten sposób, każda wiadomość, nawet zawierająca dokładnie taką samą transakcję, jest inna.

Numer	Kto otrzyma	Kto zapłaci	Ile	Podpis
1	Aurora	Dzierżykraj	15	Dzierżykraj
2	Beatrycze	Aurora	10	Aurora
3	Cieszygor	Beatrycze	50	Beatrycze
4	Dzierżykraj	Beatrycze	5	Beatrycze

Dziennik transakcji

Wystarczy na początku do wiadomości opisującej transakcję dodać jej numer. W ten sposób, każda wiadomość, nawet zawierająca dokładnie taką samą transakcję, jest inna.

Numer	Kto otrzyma	Kto zapłaci	Ile	Podpis
1	Aurora	Dzierżykraj	15	Dzierżykraj
2	Beatrycze	Aurora	10	Aurora
3	Cieszygor	Beatrycze	50	Beatrycze
4	Dzierżykraj	Beatrycze	5	Beatrycze

Kolejny problem: jak zmusić ludzi, by spłacili zobowiązania na żądanie? Mogą przecież obiecać wysokie płatności w rozliczeniu, a potem się nie rozliczyć?

Sposób rozliczenia

Sposób rozliczenia

- W protokole kryptowalut cykl transakcji zaczyna się od wpłacenia przez użytkowników pewnych kwot do puli (np. po 1000 złotych) i dopisania do dziennika rozliczeń kilku początkowych transakcji stwierdzających, że każdy ma prawo taką kwotę otrzymać z puli.

Sposób rozliczenia

- W protokole kryptowalut cykl transakcji zaczyna się od wpłacenia przez użytkowników pewnych kwot do puli (np. po 1000 złotych) i dopisania do dziennika rozliczeń kilku początkowych transakcji stwierdzających, że każdy ma prawo taką kwotę otrzymać z puli.
- Protokół nie akceptuje transakcji, w wyniku których ktoś wydaje więcej niż ma na liście wpłat.

Sposób rozliczenia

- W protokole kryptowalut cykl transakcji zaczyna się od wpłacenia przez użytkowników pewnych kwot do puli (np. po 1000 złotych) i dopisania do dziennika rozliczeń kilku początkowych transakcji stwierdzających, że każdy ma prawo taką kwotę otrzymać z puli.
- Protokół nie akceptuje transakcji, w wyniku których ktoś wydaje więcej niż ma na liście wpłat.
- Ten krok usuwa konieczność rozliczenia i powiązanie dziennika transakcji z jakąkolwiek walutą - uczestnicy, jeśli tylko chcą, mogą już zawsze posługiwać się tylko dziennikiem do rozliczeń.

Sposób rozliczenia

Numer	Kto otrzyma	Kto zapłaci	Ile	Podpis
1	Aurora	System	1000	System
2	Beatrycze	System	1000	System
3	Cieszygor	System	1000	System
4	Dzierżykraj	System	1000	System
5	Aurora	Cieszygor	500	Cieszygor
6	Beatrycze	Cieszygor	200	Cieszygor
7	Dzierżykraj	Cieszygor	400	Cieszygor

Ostatnia transakcja nie zostanie zaakceptowana przez system, póki ktoś nie obieca zapłacić Cieszygorowi.

Decentralizacja

Decentralizacja: brak organu nadzorującego i monitorującego transakcje.

Decentralizacja

Decentralizacja: brak organu nadzorującego i monitorującego transakcje.

- No ale... ktoś ten „dziennik” ma i może go kontrolować?

Decentralizacja

Decentralizacja: brak organu nadzorującego i monitorującego transakcje.

- No ale... ktoś ten „dziennik” ma i może go kontrolować?
- Każdy użytkownik posiada własną kopię dziennika! By doszło do transakcji, użytkownik musi ją ujawnić całej sieci i wszyscy mogą zaktualizować swoje wersje dziennika.

Decentralizacja

Decentralizacja: brak organu nadzorującego i monitorującego transakcje.

- No ale... ktoś ten „dziennik” ma i może go kontrolować?
- Każdy użytkownik posiada własną kopię dziennika! By doszło do transakcji, użytkownik musi ją ujawnić całej sieci i wszyscy mogą zaktualizować swoje wersje dziennika.
- Najtrudniejszy krok: jak sprawić, by dzienniki transakcji wszystkich użytkowników były zgodne (przynajmniej na dłuższą metę).

Decentralizacja

Decentralizacja: brak organu nadzorującego i monitorującego transakcje.

- No ale... ktoś ten „dziennik” ma i może go kontrolować?
- Każdy użytkownik posiada własną kopię dziennika! By doszło do transakcji, użytkownik musi ją ujawnić całej sieci i wszyscy mogą zaktualizować swoje wersje dziennika.
- Najtrudniejszy krok: jak sprawić, by dzienniki transakcji wszystkich użytkowników były zgodne (przynajmniej na dłuższą metę).
- Odpowiedź: protokół *blockchain*.

Idea

Pomysł: najwiarygodniejszy dziennik to taki, w którego stworzenie włożono najwięcej mocy obliczeniowej.

Idea

Pomysł: najwiarygodniejszy dziennik to taki, w którego stworzenie włożono najwięcej mocy obliczeniowej.

- Transakcje grupujemy w zestawy (bloki).

Idea

Pomysł: najwiarygodniejszy dziennik to taki, w którego stworzenie włożono najwięcej mocy obliczeniowej.

- Transakcje grupujemy w zestawy (bloki).
- Zaakceptowanie zestawu transakcji wymaga odgadnięcia pewnego kodu, którego wyznaczenie wymaga włożenia dużej mocy obliczeniowej.

Idea

Pomysł: najwiarygodniejszy dziennik to taki, w którego stworzenie włożono najwięcej mocy obliczeniowej.

- Transakcje grupujemy w zestawy (bloki).
- Zaakceptowanie zestawu transakcji wymaga odgadnięcia pewnego kodu, którego wyznaczenie wymaga włożenia dużej mocy obliczeniowej.
- Jeśli większość mocy obliczeniowej w sieci nie potwierdza zestawu transakcji, nie jest on akceptowany.

Idea

Pomysł: najwiarygodniejszy dziennik to taki, w którego stworzenie włożono najwięcej mocy obliczeniowej.

- Transakcje grupujemy w zestawy (bloki).
- Zaakceptowanie zestawu transakcji wymaga odgadnięcia pewnego kodu, którego wyznaczenie wymaga włożenia dużej mocy obliczeniowej.
- Jeśli większość mocy obliczeniowej w sieci nie potwierdza zestawu transakcji, nie jest on akceptowany.
- Na dłuższą metę, utrzymanie fałszywego zestawu transakcji „w obiegu” przez małą grupę oszustów nie jest możliwe.

Funkcja skrótu (haszująca)

Funkcja skrótu (haszująca)

- Funkcja skrótu (haszująca) przekształca dowolne teksty w ciągi zer i jedynek o zadanej długości zwane skrótami nieodwracalnymi (*hash*, *digest*). Najpopularniejsza funkcja skrótu SHA256 tworzy ciągi o długości 256 znaków.

Funkcja skrótu (haszująca)

- Funkcja skrótu (haszująca) przekształca dowolne teksty w ciągi zer i jedynek o zadanej długości zwane skrótami nieodwracalnymi (*hash*, *digest*). Najpopularniejsza funkcja skrótu SHA256 tworzy ciągi o długości 256 znaków.
- Mała zmiana tekstu powoduje dużą zmianę wyniku (utrudnia rozkodowanie): znowu algorytmy kryptologiczne!

Funkcja skrótu (haszująca)

- Funkcja skrótu (haszująca) przekształca dowolne teksty w ciągi zer i jedynek o zadanej długości zwane skrótami nieodwracalnymi (*hash*, *digest*). Najpopularniejsza funkcja skrótu SHA256 tworzy ciągi o długości 256 znaków.
- Mała zmiana tekstu powoduje dużą zmianę wyniku (utrudnia rozkodowanie): znowu algorytmy kryptologiczne!
- Kryptograficzne funkcje skrótu są używane nie tylko w kryptowalutach - niemal każda zaszyfrowana komunikacja używa jednej z tych funkcji.

Dowód wykonania pracy

Dowód wykonania pracy

- Każdy wysyła w sieć informacje o swoich transakcjach, by wpisać je do „globalnego” dziennika.

Dowód wykonania pracy

- Każdy wysyła w sieć informacje o swoich transakcjach, by wpisać je do „globalnego” dziennika.
- Dziennik transakcji jest dzielony na bloki, zawierające ustaloną liczbę transakcji (dla bitcoina - 2400) z dodatkową liczbą na końcu zwaną „dowodem wykonania pracy” (proof-of-work). Jest to taka liczba, że wartość całego bloku po przekształceniu przez funkcję skrótu, zaczyna się od ustalonej liczby (np. 30) zer.

Dowód wykonania pracy

- Każdy wysyła w sieć informacje o swoich transakcjach, by wpisać je do „globalnego” dziennika.
- Dziennik transakcji jest dzielony na bloki, zawierające ustaloną liczbę transakcji (dla bitcoina - 2400) z dodatkową liczbą na końcu zwaną „dowodem wykonania pracy” (proof-of-work). Jest to taka liczba, że wartość całego bloku po przekształceniu przez funkcję skrótu, zaczyna się od ustalonej liczby (np. 30) zer.
- Blok, zawierający transakcje znane odbiorcy, jest akceptowalny, jeśli faktycznie jego proof-of-work jest prawidłowy. Sprawdzenie tego jest bardzo łatwe - wystarczy zastosować do proof-of-work funkcję skrótu.

Dowód wykonania pracy

- Każdy wysyła w sieć informacje o swoich transakcjach, by wpisać je do „globalnego" dziennika.
- Dziennik transakcji jest dzielony na bloki, zawierające ustaloną liczbę transakcji (dla bitcoina - 2400) z dodatkową liczbą na końcu zwaną „dowodem wykonania pracy" (proof-of-work). Jest to taka liczba, że wartość całego bloku po przekształceniu przez funkcję skrótu, zaczyna się od ustalonej liczby (np. 30) zer.
- Blok, zawierający transakcje znane odbiorcy, jest akceptowalny, jeśli faktycznie jego proof-of-work jest prawidłowy. Sprawdzenie tego jest bardzo łatwe - wystarczy zastosować do proof-of-work funkcję skrótu.
- Natomiast znalezienie proof-of-work na podstawie wyniku jest obliczeniowo ciężkie, gdyż wymaga 2^{30}, czyli około miliard operacji skrótu).

Blockchain

Blockchain

- Kolejność bloku w łańcuchu: dołączany blok musi na początku zawierać wynik funkcji skrótu bloku poprzedniego (co musi być uwzględnione w obliczeniach kolejnego proof-of-work) i nie powtarzać transakcji z bloków poprzednich. W ten sposób powstaje *blockchain*: „łańcuch bloków”.

Blockchain

- Kolejność bloku w łańcuchu: dołączany blok musi na początku zawierać wynik funkcji skrótu bloku poprzedniego (co musi być uwzględnione w obliczeniach kolejnego proof-of-work) i nie powtarzać transakcji z bloków poprzednich. W ten sposób powstaje *blockchain*: „łańcuch bloków”.
- Stabilność łańcucha: zmiana dawnej transakcji w którymś z dawno zaakcpetowanych bloków zmienia proof-of-work i w konsekwencji wszystkie kolejne bloki.

Blockchain

- Kolejność bloku w łańcuchu: dołączany blok musi na początku zawierać wynik funkcji skrótu bloku poprzedniego (co musi być uwzględnione w obliczeniach kolejnego proof-of-work) i nie powtarzać transakcji z bloków poprzednich. W ten sposób powstaje *blockchain*: „łańcuch bloków".
- Stabilność łańcucha: zmiana dawnej transakcji w którymś z dawno zaakcpetowanych bloków zmienia proof-of-work i w konsekwencji wszystkie kolejne bloki.
- Jedyny sposób sfałszowania transakcji ujętej w blockchain: wykonanie proof-of-work dla wszystkich fałszywych bloków szybciej, niż pozostali użytkownicy tworzą nowe bloki łańcucha.

Nagrody dla kopaczy

Nagrody dla kopaczy

- Każdy może tworzyć i proponować do akceptacji w sieci bloki transakcji. Taka osoba zbiera informacje o transakcjach wysyłane przez użytkowników, dowolnie je „blokuje”, wybiera łańcuch do którego chce blok dołączyć i próbuje wyznaczyć proof-of-work szybciej niż inni. Jeśli się uda, wysyła „w sieć” informację o stworzonym bloku.

Nagrody dla kopaczy

- Każdy może tworzyć i proponować do akceptacji w sieci bloki transakcji. Taka osoba zbiera informacje o transakcjach wysyłane przez użytkowników, dowolnie je „blokuje”, wybiera łańcuch do którego chce blok dołączyć i próbuje wyznaczyć proof-of-work szybciej niż inni. Jeśli się uda, wysyła „w sieć” informację o stworzonym bloku.
- Po co? Twórca bloku może do niego dodać, jako nagrodę, jedną transakcję, która mówi, że dostaje on „znikąd” pewną ustaloną z góry kwotę. To jedyny typ transakcji, który nie musi być podpisany.

Nagrody dla kopaczy

- Każdy może tworzyć i proponować do akceptacji w sieci bloki transakcji. Taka osoba zbiera informacje o transakcjach wysyłane przez użytkowników, dowolnie je „blokuje”, wybiera łańcuch do którego chce blok dołączyć i próbuje wyznaczyć proof-of-work szybciej niż inni. Jeśli się uda, wysyła „w sieć” informację o stworzonym bloku.
- Po co? Twórca bloku może do niego dodać, jako nagrodę, jedną transakcję, która mówi, że dostaje on „znikąd” pewną ustaloną z góry kwotę. To jedyny typ transakcji, który nie musi być podpisany.
- Ta nagroda to zazwyczaj jedyny sposób „kreacji pieniądza” w ramach kryptowaluty, dlatego tworzenie bloków nazywane jest „kopaniem” (*mining*), a sami twórcy „cyfrowymi górnikami” lub „kopaczami”.

Tworzenie bloków, a użytkownicy sieci

Tworzenie bloków, a użytkownicy sieci

- Poza cyfrowymi górnikami, użytkownicy nie muszą już zbierać informacji o transakcjach, a jedynie o łańcuchach bloków.

Tworzenie bloków, a użytkownicy sieci

- Poza cyfrowymi górnikami, użytkownicy nie muszą już zbierać informacji o transakcjach, a jedynie o łańcuchach bloków.
- Jeśli ktoś otrzymuje informacje o dwóch sprzecznych łańcuchach bloków, wierzy temu, który jest dłuższy, czyli stoi za nim więcej mocy obliczeniowej. Gdy dwa są równie długie, czekamy na dalsze informacje - dość szybko jedna z historii okaże się „mniej wiarygodna" dla większości sieci i wspólny dziennik transakcji się ustabilizuje.

Tworzenie bloków, a użytkownicy sieci

- Poza cyfrowymi górnikami, użytkownicy nie muszą już zbierać informacji o transakcjach, a jedynie o łańcuchach bloków.
- Jeśli ktoś otrzymuje informacje o dwóch sprzecznych łańcuchach bloków, wierzy temu, który jest dłuższy, czyli stoi za nim więcej mocy obliczeniowej. Gdy dwa są równie długie, czekamy na dalsze informacje - dość szybko jedna z historii okaże się „mniej wiarygodna" dla większości sieci i wspólny dziennik transakcji się ustabilizuje.
- Nie ma potrzeby ufania jakiejkolwiek pojedynczej osobie lub instytucji!

Co musiałby zrobić oszust?

Co musiałby zrobić oszust?

- Aurora chce oszukać Cieszygora tworząc dla niego fałszywy blok, potwierdzający transakcję, w której przelewa mu 100, ale nie wysyła jej do reszty sieci, licząc, że dzięki temu zaoszczędzi i nie będzie przyłapana. Inni o transakcji nie wiedzą.

Co musiałby zrobić oszust?

- Aurora chce oszukać Cieszygora tworząc dla niego fałszywy blok, potwierdzający transakcję, w której przelewa mu 100, ale nie wysyła jej do reszty sieci, licząc, że dzięki temu zaoszczędzi i nie będzie przyłapana. Inni o transakcji nie wiedzą.
- By w ogóle taki blok gdziekolwiek został potwierdzony, Aurora musi wykonać dowód pracy szybciej niż pozostali górnicy stworzą bloki zawierające inne transakcje z jej bloku. Powiedzmy, że ma na tyle dużą moc obliczeniową, że prawdopodobieństwo, że jej się uda wynosi $\frac{1}{4}$.

Co musiałby zrobić oszust?

- Aurora chce oszukać Cieszygora tworząc dla niego fałszywy blok, potwierdzający transakcję, w której przelewa mu 100, ale nie wysyła jej do reszty sieci, licząc, że dzięki temu zaoszczędzi i nie będzie przyłapana. Inni o transakcji nie wiedzą.
- By w ogóle taki blok gdziekolwiek został potwierdzony, Aurora musi wykonać dowód pracy szybciej niż pozostali górnicy stworzą bloki zawierające inne transakcje z jej bloku. Powiedzmy, że ma na tyle dużą moc obliczeniową, że prawdopodobieństwo, że jej się uda wynosi $\frac{1}{4}$.
- Nikt z innych górników nie ma fałszywej transakcji w swoim spisie, więc nikt poza Aurorą nie może sprawdzić funkcji skrótu dla jej bloku i kontynuować jej łańcuch bloków. Pozostali pracują na innych łańcuchach i wkrótce stworzą kolejny blok, wydłużający ich łańcuch poza ten stworzony przez Aurorę.

Co musiałby zrobić oszust?

Co musiałby zrobić oszust?

- Nikt z innych górników nie ma fałszywej transakcji w swoim spisie, więc nikt poza Aurorą nie może sprawdzić funkcji skrótu dla jej bloku i kontynuować jej łańcuch bloków. Pozostali pracują na innych łańcuchach i wkrótce stworzą kolejny blok, wydłużający ich łańcuch poza ten stworzony przez Aurorę.

Co musiałby zrobić oszust?

- Nikt z innych górników nie ma fałszywej transakcji w swoim spisie, więc nikt poza Aurorą nie może sprawdzić funkcji skrótu dla jej bloku i kontynuować jej łańcuch bloków. Pozostali pracują na innych łańcuchach i wkrótce stworzą kolejny blok, wydłużający ich łańcuch poza ten stworzony przez Aurorę.
- By Aurora znów ich wyprzedziła ze swoim kolejnym blokiem, musi znowu wygrać „wyścig" o najdłuższy istniejący łańcuch bloków. Prawdopodobieństwo, że Aurora będzie wysyłać najdłuższą historię staje się z czasem coraz mniejsze, a na dłuższą metę - praktycznie zerowe. W końcu blockchain Aurory przestanie być akceptowany (również przez Cieszygora).

Wiarygodność blockchaina i opóźnienia

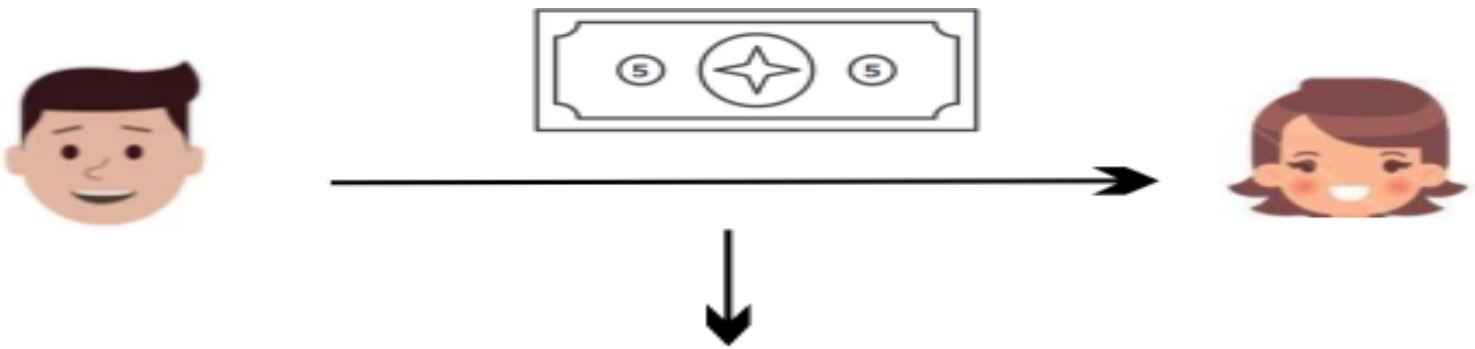
Wiarygodność blockchaina i opóźnienia

- Z powodu teoretycznej możliwości takich prób oszustw, większość programów do obsługi kryptowalut nie akceptuje nowych bloków łańcucha od razu, a czeka na potwierdzenie, że są one częścią najdłuższej historii.

Wiarygodność blockchaina i opóźnienia

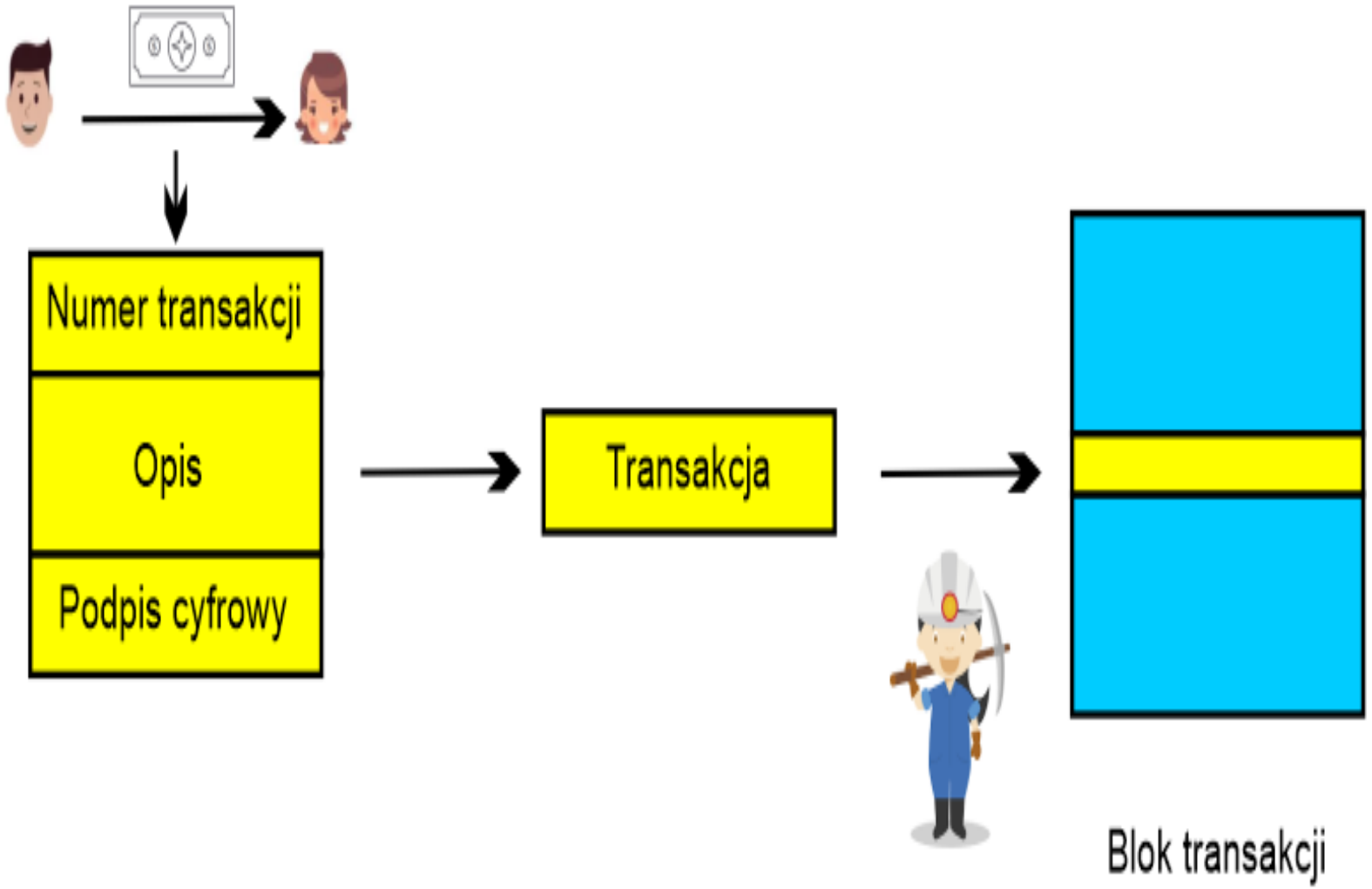
- Z powodu teoretycznej możliwości takich prób oszustw, większość programów do obsługi kryptowalut nie akceptuje nowych bloków łańcucha od razu, a czeka na potwierdzenie, że są one częścią najdłuższej historii.
- Jeśli ktoś chce by jego transakcja była szczególnie szybko zaktualizowana, może do niej dorzucić opcjonalną dodatkową opłatę dla górnika, zachęcając go do zawarcia jej w swoim bloku.

Transakcja

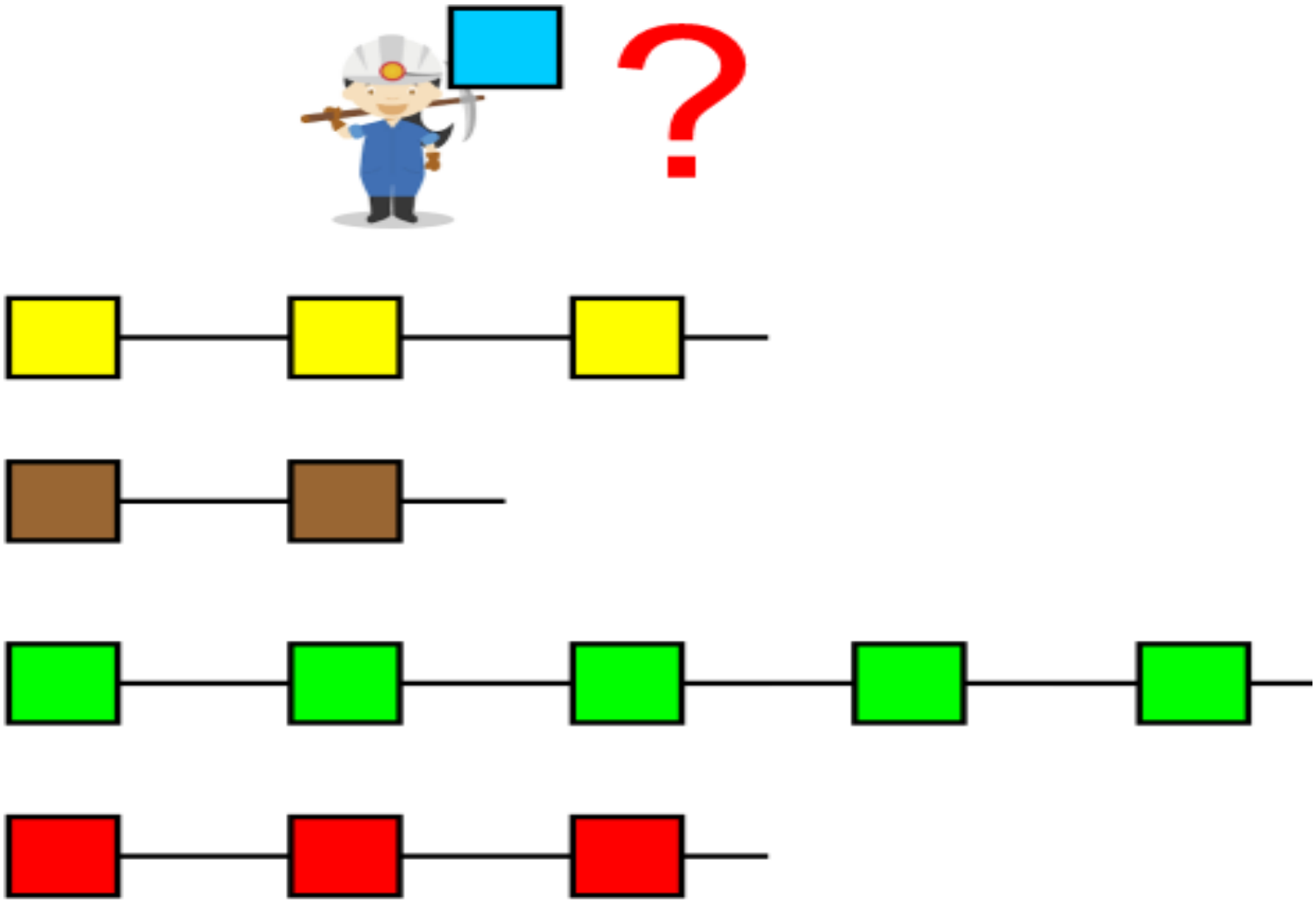


Numer transakcji
Opis
Podpis cyfrowy

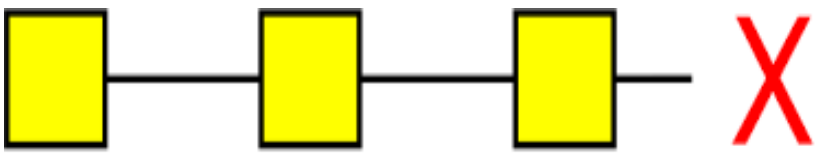
Blok transakcji

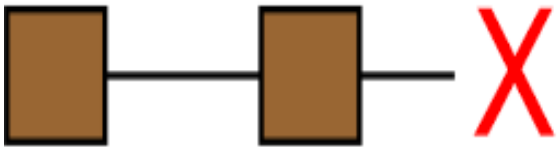


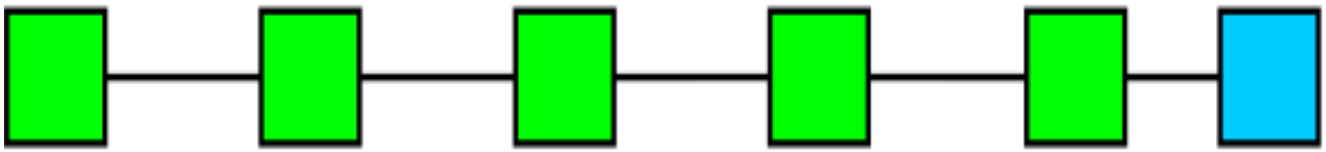
Konkurencyjne łańcuchy

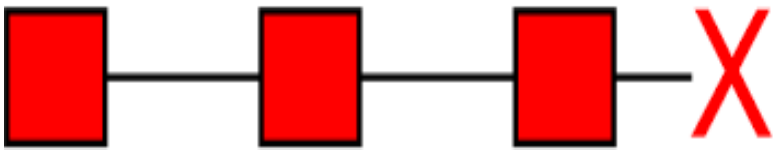


Wybór łańcucha

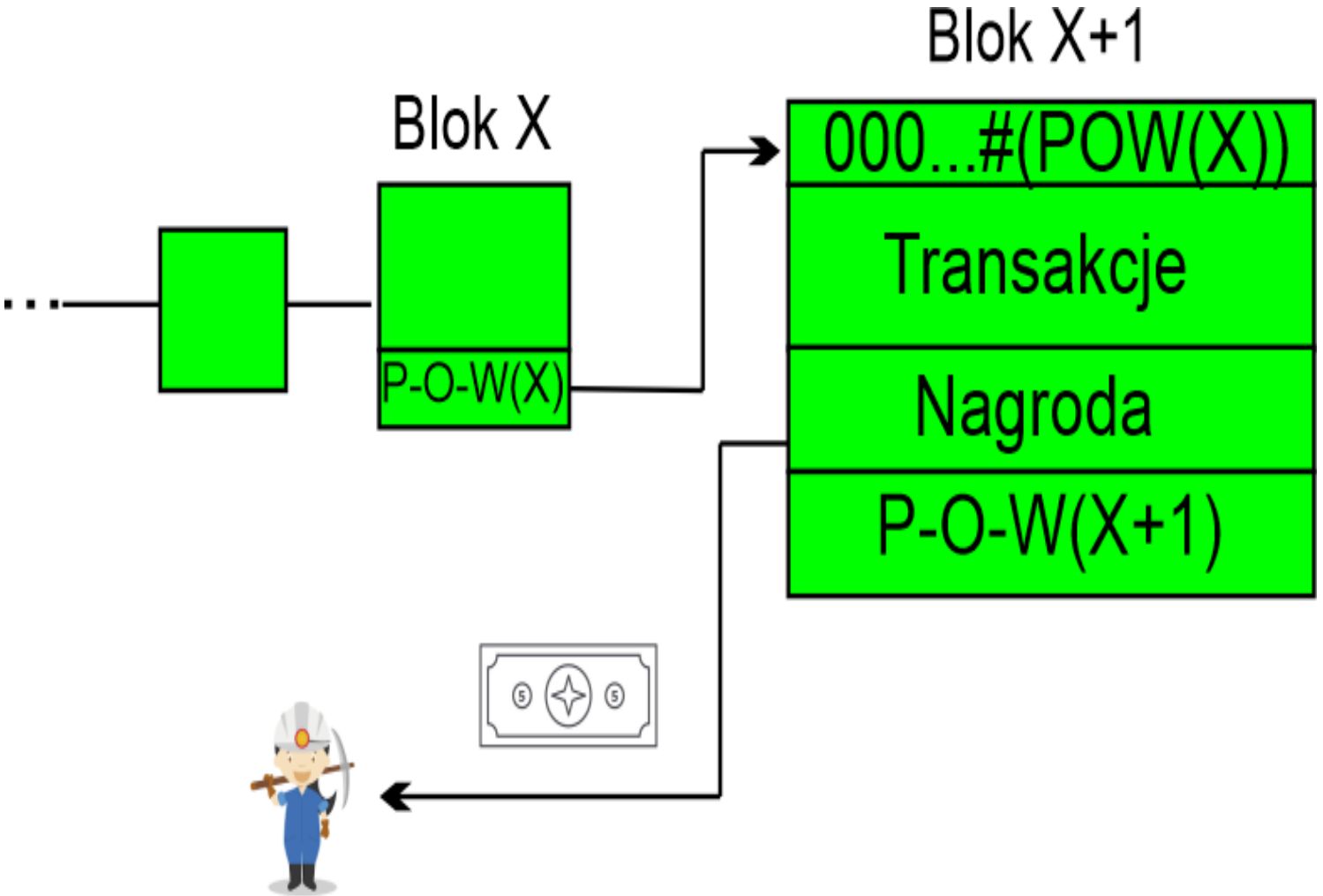








Dowód pracy i wynagrodzenie



Podsumowanie obrony przed błędami i oszustwami

- Dopisanie fałszywej korzystnej transakcji blokuje podpis cyfrowy.

Podsumowanie obrony przed błędami i oszustwami

- Dopisanie fałszywej korzystnej transakcji blokuje podpis cyfrowy.
- Wieczne zadłużanie się - nie jest możliwe ze względu na konieczność wpłaty początkowej.

Podsumowanie obrony przed błędami i oszustwami

- Dopisanie fałszywej korzystnej transakcji blokuje podpis cyfrowy.
- Wieczne zadłużanie się - nie jest możliwe ze względu na konieczność wpłaty początkowej.
- Sfałszowanie już zatwierdzonej historii blokuje system dowodów pracy i funkcji skrótu.

Podsumowanie obrony przed błędami i oszustwami

- Dopisanie fałszywej korzystnej transakcji blokuje podpis cyfrowy.
- Wieczne zadłużanie się - nie jest możliwe ze względu na konieczność wpłaty początkowej.
- Sfałszowanie już zatwierdzonej historii blokuje system dowodów pracy i funkcji skrótu.
- Stworzenie nieprawidłowego bloku i dopisanie go do łańcucha jest możliwe krótkoterminowo, ale długoterminowo łańcuch z nieprawidłowym blokiem nie będzie kontynuowany i zniknie z dziennika transakcji.

Podsumowanie obrony przed błędami i oszustwami

- Dopisanie fałszywej korzystnej transakcji blokuje podpis cyfrowy.
- Wieczne zadłużanie się - nie jest możliwe ze względu na konieczność wpłaty początkowej.
- Sfałszowanie już zatwierdzonej historii blokuje system dowodów pracy i funkcji skrótu.
- Stworzenie nieprawidłowego bloku i dopisanie go do łańcucha jest możliwe krótkoterminowo, ale długoterminowo łańcuch z nieprawidłowym blokiem nie będzie kontynuowany i zniknie z dziennika transakcji.
- Wszyscy uczestnicy systemu (dopóki nie mają „przewagi obliczeniowej") są wynagradzani za wspieranie jego poprawnego działania.

Bitcoin i regulowanie kreacji kryptowaluty

Bitcoin i regulowanie kreacji kryptowaluty

- W przypadku bitcoina, proof-of-work na początku faktycznie miał być taki, by funkcja skrótu bloku zaczynała się od 30 zer. Co jakiś czas, w miarę wzrostu mocy obliczeniowej w sieci tej kryptowaluty, liczba tych zer się zwiększa tak, by znajdowanie nowego proof-of-work i dołączanie nowego bloku do dziennika trwało około 10 minut.

Bitcoin i regulowanie kreacji kryptowaluty

- W przypadku bitcoina, proof-of-work na początku faktycznie miał być taki, by funkcja skrótu bloku zaczynała się od 30 zer. Co jakiś czas, w miarę wzrostu mocy obliczeniowej w sieci tej kryptowaluty, liczba tych zer się zwiększa tak, by znajdowanie nowego proof-of-work i dołączanie nowego bloku do dziennika trwało około 10 minut.
- Nowsze kryptowaluty używają znacznie krótszego czasu, co wydaje się wystarczająco bezpieczne (ethereum - 15 sekund, litecoin - 2,5 minuty, ripple - 3,5 sekundy).

Bitcoin i regulowanie kreacji kryptowaluty

- W przypadku bitcoina, proof-of-work na początku faktycznie miał być taki, by funkcja skrótu bloku zaczynała się od 30 zer. Co jakiś czas, w miarę wzrostu mocy obliczeniowej w sieci tej kryptowaluty, liczba tych zer się zwiększa tak, by znajdowanie nowego proof-of-work i dołączanie nowego bloku do dziennika trwało około 10 minut.
- Nowsze kryptowaluty używają znacznie krótszego czasu, co wydaje się wystarczająco bezpieczne (ethereum - 15 sekund, litecoin - 2,5 minuty, ripple - 3,5 sekundy).
- Dodatkowo, co jakiś czas, z góry zdefiniowany wielkością „wydobycia” (co 210 tysięcy bloków w przypadku bitcoina), nagrody za „kopanie” stają się o połowę mniejsze. Dzięki temu, zgodnie ze znanymi wynikami na temat ciągów geometrycznych, liczba bitcoinów jest ograniczona z góry (przez 21 milionów).

Dziękuję za uwagę.

grzegorz.kosiorowski@uek.krakow.pl