Sem:BK: Blockchain

Norbert J.

Instytut Informatyki, Uniwersytet Wrocławski

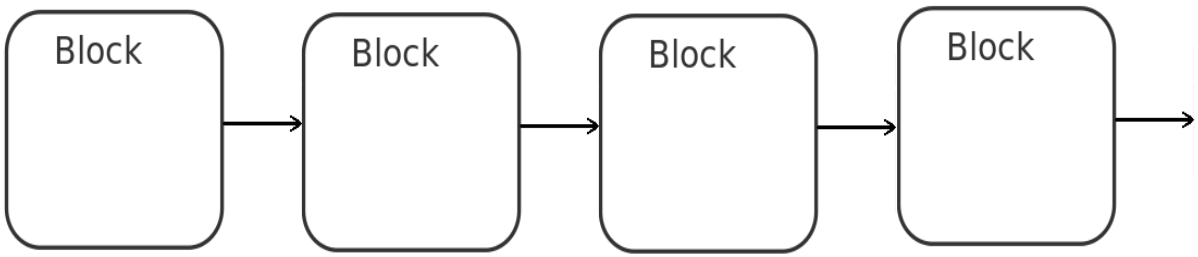
18 kwietnia 2018

Spis treści

1 Wstęp
2 Bitcoin
3 Ethereum
4 Nie proof-of-work
5 Ataki
6 Wykresy
7 Podsumowanie

Intuicja

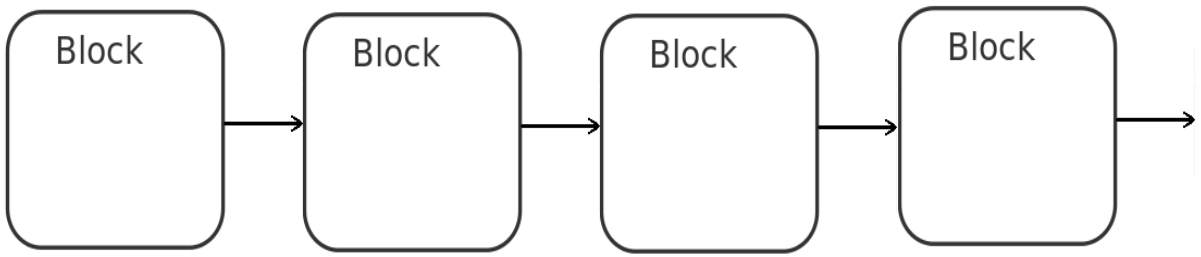
Co to jest blockchain?



łańcuch bloków

Intuicja

Co to jest blockchain?



łańcuch bloków

To prawda, ale blockchain jest nieco bardziej skomplikowany.

Tak naprawdę

Czym jest blockchain?

- Ogólnodostępny przez p2p (zazwyczaj)
- Zabezpieczony kryptograficznie
  (nie można go łatwo sfałszować/zmienić)
- Łańcuch bloków
- Używany początkowo w Bitcoinie do potwierdzania transakcji.

Będę opisywał blockchain głównie na przykładzie Bitcoina.

Spis treści

1 Wstęp

2 Bitcoin

3 Ethereum

4 Nie proof-of-work

5 Ataki

6 Wykresy

7 Podsumowanie

Główny problem: Double spending

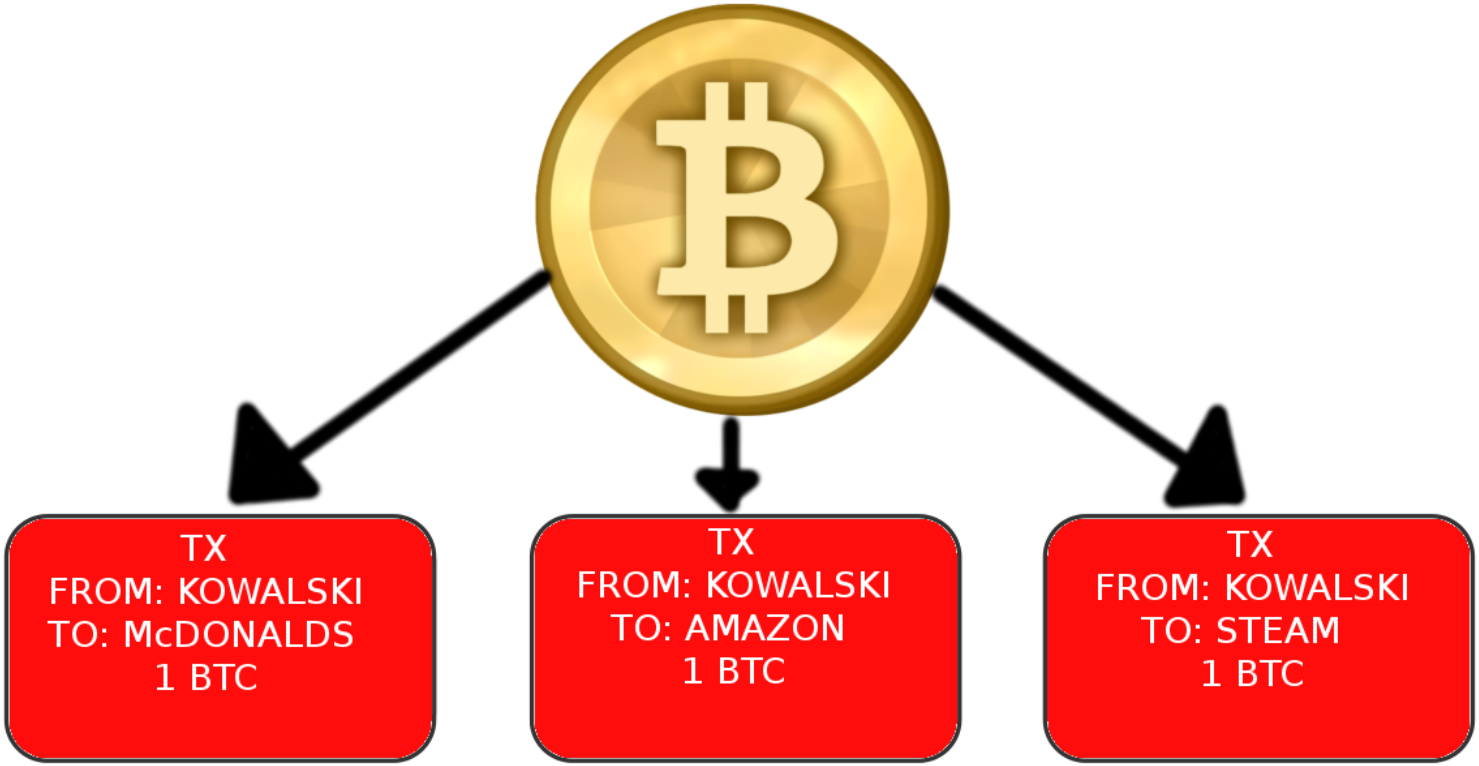
Największym problemem podczas tworzenia Bitcoina było wielokrotne wydawanie wirtualnych pieniędzy.

W świecie **rzeczywistym** łatwiej stwierdzić gdzie dana rzecz się znajduje.
W świecie **wirtualnym** możemy kopiować rzeczy, pieniądze. Chyba, że bank nam zabroni.
Co jeśli **banku** – centralnej jednostki zarządzającej – nie ma?

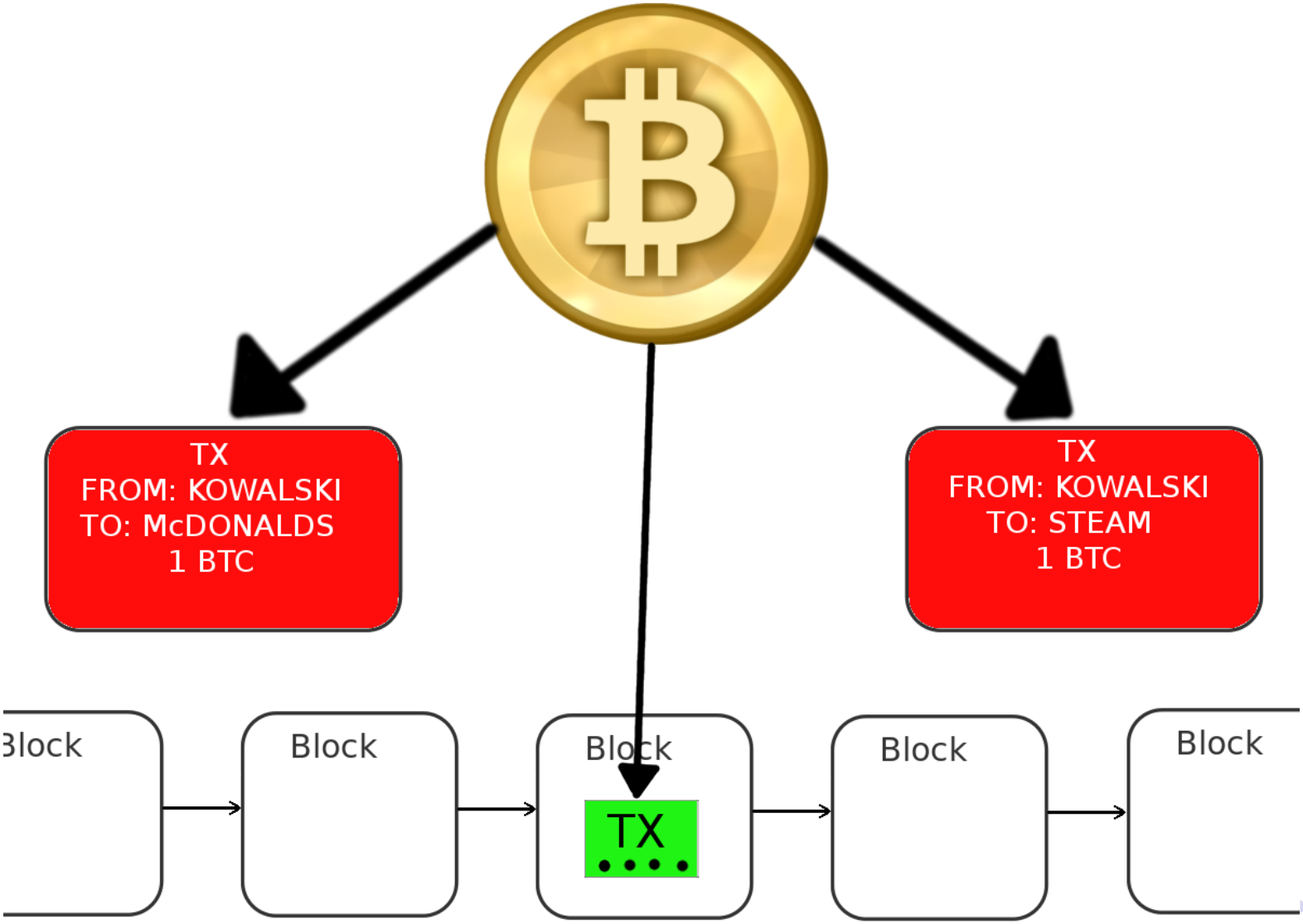
Bitcoin jest w pełni **rozproszonym** systemem płatności (nie ma centralnej jednostki)

Dzięki blockchainowi udało się rozwiązać ten problem.

Która transakcja jest tą prawidłową?



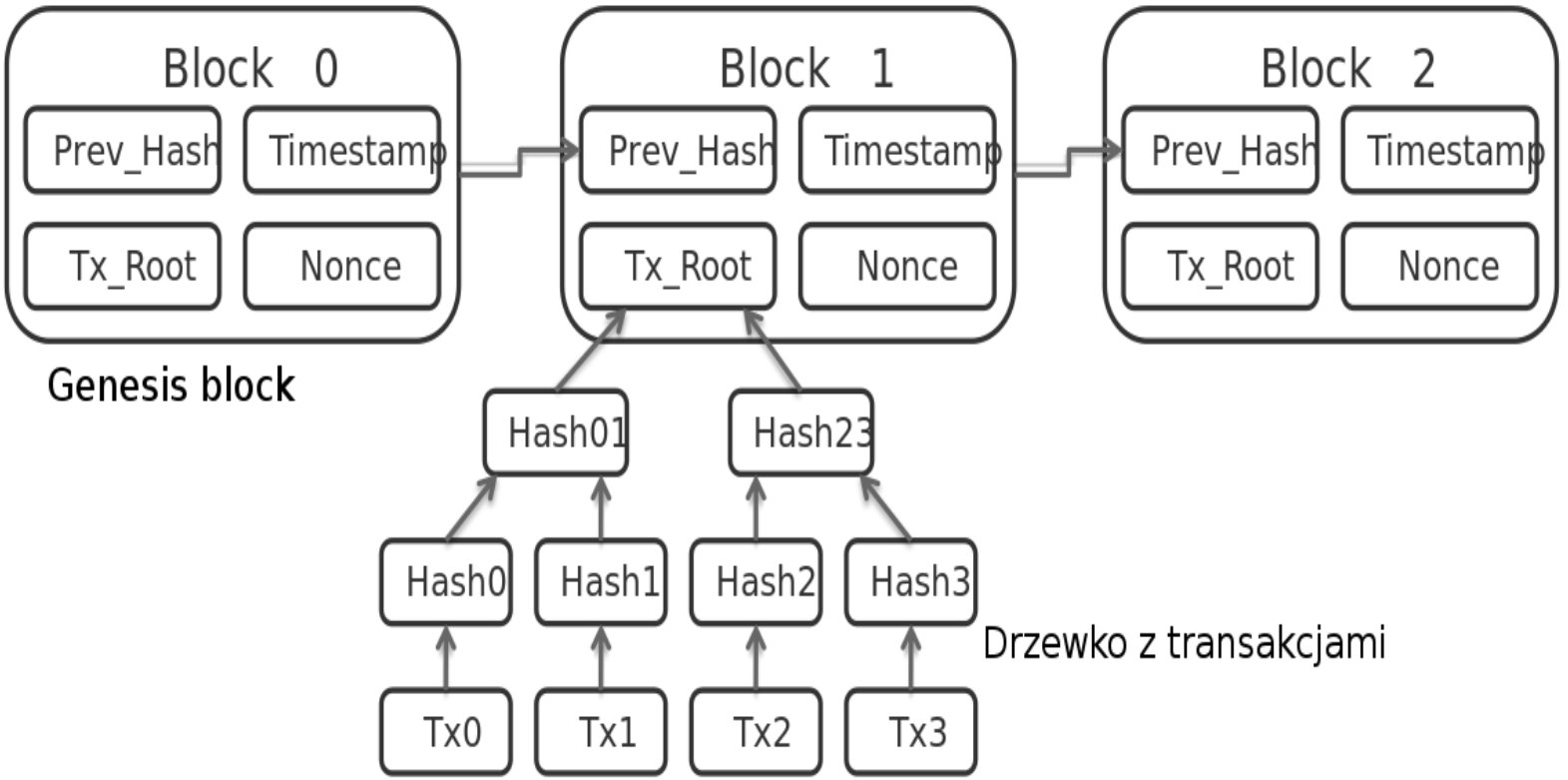
Która transakcja jest tą prawidłową? Ta w blockchainie!



Zasada potwierdzania w Bitcoinie

- Jest **jeden poprawny główny łańcuch bloków** od najstarszego do najnowszego
  (z dokładnością do kilku najnowszych bloków)
- Transakcja będąca w tym poprawnym ciągu bloków jest uznana za potwierdzoną
- Wszystko w nowym bloku musi być spójne z poprzednimi blokami
  - nie ma możliwości double-spendingu
  - Kowalski tylko raz może wydać i tylko swoje pieniądze

Schemat



Mogę pokazać dokładniej co znajduje się w bloku.

Genesis block

Genesis block to pierwszy blok blockchaina.

Nie można go zmienić.

To jest umowa, że pierwszy jest ten konkretny blok.

Składowe bloku

- **Prev_Hash** – hash poprzedniego bloku.
- **Timestamp** – czas wykopania.
  Musi być większy niż średnia ostatnich 11 timestampów.
  Nie musi być dokładny.
- **Tx_Root** – drzewko Merkle z transakcjami (w Bitcoinie).
  Ogólnie jakieś dane, które chcemy wykopywać.
- **Nonce** – dowolny ciąg znaków ustalonej długości.
  Bardzo pomocny przy kopaniu.

Kopanie bloku, czyli Proof-of-work

Czym jest kopanie?
Znalezieniem nowego, spójnego z poprzednimi bloku, którego **hash** (SHA256) będzie **odpowiednio mały**.

Czemu jest to trudne?
Hash oblicza się łatwo **w jedną stronę**.
Mając dany tekst, prosto znaleźć jego hash.
Mając hash, do którego ma się hashować blok, trudno znaleźć cokolwiek innego, co hashuje się do niego.

Jak się kopie?
1. Ustalamy podstawowe parametry bloku (Prev_Hash, Tx_root jak i całe drzewo transakcji, ...)
2. Zmieniając **Timestamp** i **Nonce**, hashujemy kolejne niemal identyczne bloki. Hashe będą zupełnie inne.
3. Jak któryś hash jest odpowiednio mały => WYGRANA!!!
Wykopaliśmy poprawny blok

Kopanie bloku, czyli Proof-of-work (2)

Jak mały ma być hash?
Tak, aby cała sieć kopała średnio 1 blok na 10 min.
Co 2 tygodnie bloków (2016 bloków) obliczana jest nowa trudność.

Dlaczego niby chcemy kopać bloki?
Bo dostajemy Bitcoiny za:

- wykopanie bloku (generowanie Bitcoinów)
- potwierdzenie transakcji które umieściliśmy w bloku

czyli po prostu zarabiamy.

Trudność kopania

Target – zmienna określająca do co najwyżej jak małej wartości ma hashować się cały blok.

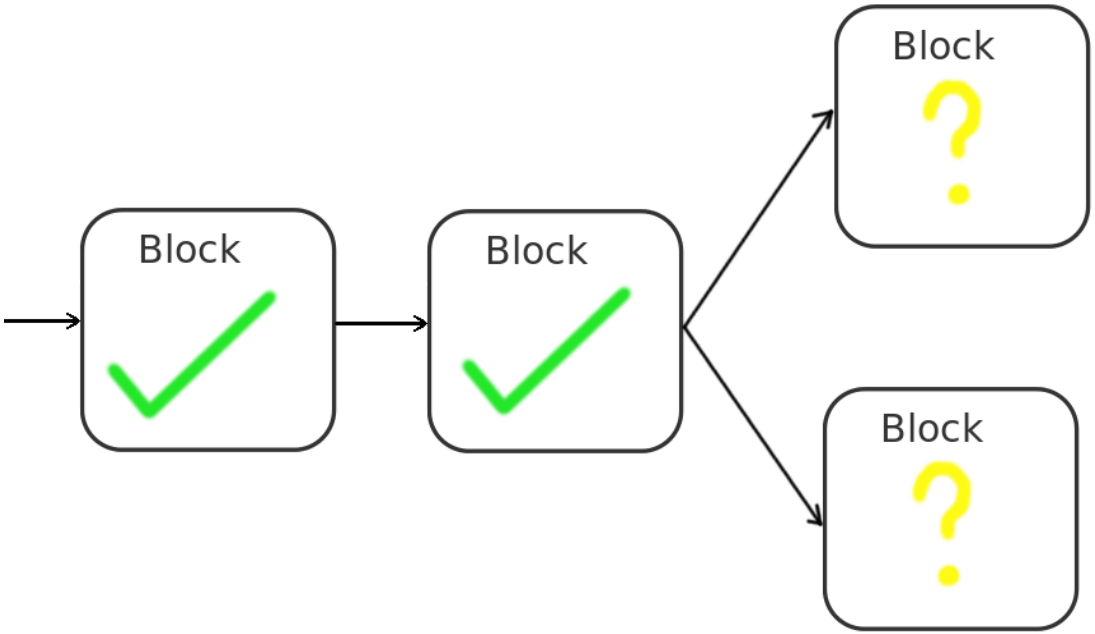
Difficulty – trudność wykopania bloku. Im większa tym trudniej.

$$difficulty = \frac{difficulty\_1\_target}{current\_target}$$

$$difficulty\_1\_target = 0x00000000FFFF0000000000000000000000000000000000000000000000000000$$

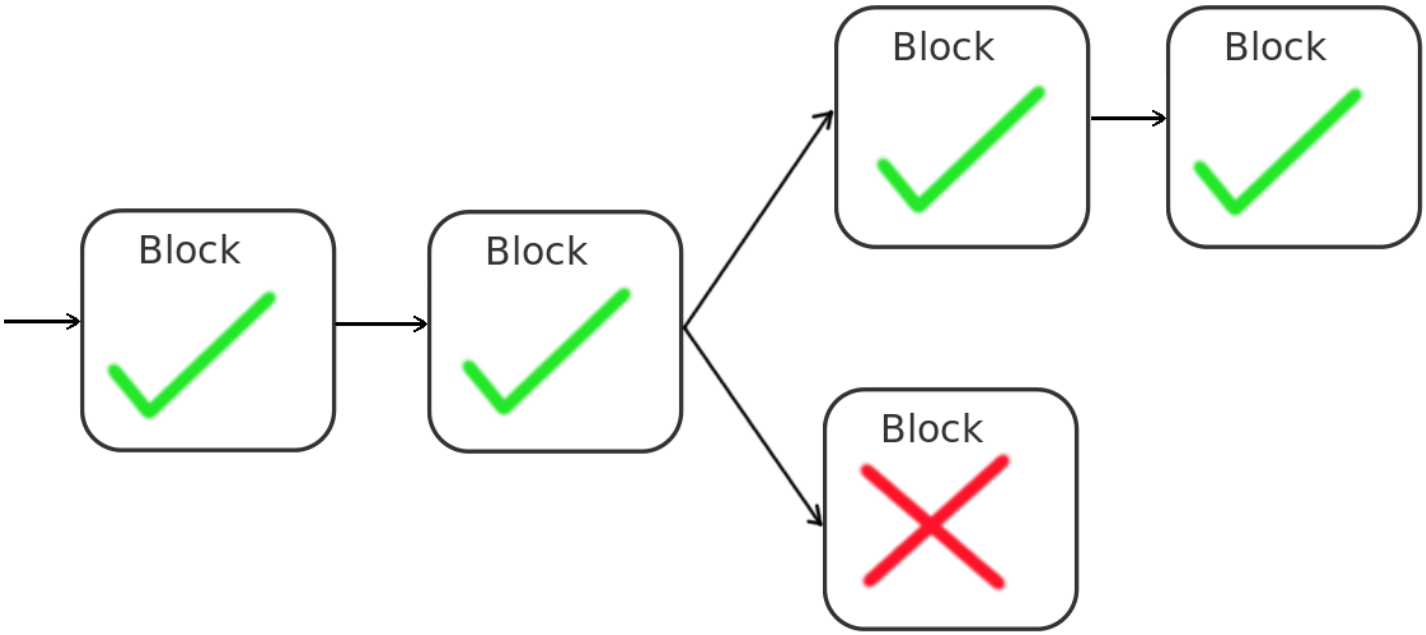
Fork (przypadkowy)

A co jeśli 2 kopaczy wykopie nowy, poprawny blok?



Fork (przypadkowy, 2)

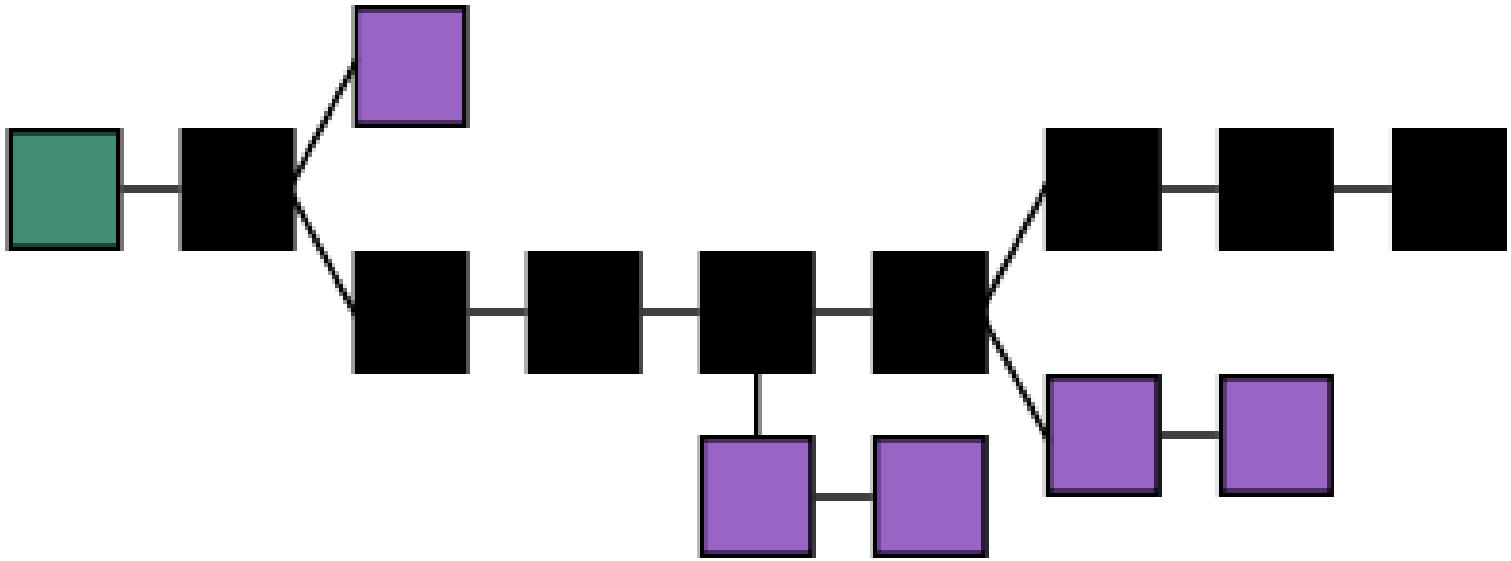
A co jeśli 2 kopaczy wykopie nowy, poprawny blok?



Nie jest to zbyt duży problem. Kopacze mogą wybrać blok do kopania.

Który ciąg bloków jest jedynym poprawnym?

Co jeśli jest więcej poprawnych bloków?



Wtedy tym jedynym jest ten **najdłuższy poprawny**.
Inne są nieistotne.
Warto poczekać, aż kilka bloków przykryje blok z naszą transakcją.

Intencyjny fork (intentional fork)

Czasem sieć potrzebuje pewnych zmian w protokole.
Wprowadza się więc forki.

Takie forki dzielimy na:

- **soft fork**
  programy sprawdzające stare reguły interpretują bloki z nowymi regułami jako poprawne (zawężenie reguł)
- **hard fork**
  programy sprawdzające stare reguły interpretują bloki z nowymi regułami jako niepoprawne (osłabienie reguł)
  cała sieć musi współpracować (przejść na nowe reguły) by się nie rozdzielić

Bitcoin soft fork z sierpnia 2010

15 sierpnia 2010 została wykopana transakcja przekręcająca licznik wydawanych BTC.

- **błąd** w procesie weryfikacji
- transakcja **wygenerowała** 184,467,440,737.09551616 BTC na 2 adresy
- transakcja została wykryta po około 1,5h
- łatka została wytworzona w 4h
- sieć się rozdwoiła
  - jedna część akceptowała blok z wadliwą transakcją
  - druga nie
- po pewnym czasie sieć nieakceptująca wadliwego bloku wyprzedziła tę akceptującą
- naturalnie sieć akceptująca **przerzuciła się** na nieakceptującą

Spis treści

1 Wstęp

2 Bitcoin

3 Ethereum

4 Nie proof-of-work

5 Ataki

6 Wykresy

7 Podsumowanie

Ethereum

- Druga najbardziej znana kryptowaluta
- Korzysta z blockchain
- Zamiast co 10 min, nowy blok co **14-15 sekund**!
- Zamiast SHA256 używa **Ethash**
- Częściowo używa proof-of-stake (będzie później)

Ethereum hard fork z lipca 2016

- 20 lipca 2016 użytkownik wykorzystał lukę w kodzie aplikacji DAO (A decentralized autonomous organization)
- ta **luka** była **poza** samym Ethereum
- uzyskał tym samym dostęp do 3,6 mln ETH, czyli "ponad 1/3 wykopanych już przez górników (nie licząc wygenerowanych na początku projektu) żetonów"
- obawiano się **niestabilności** kursu ETH w przypadku sprzedaży tych ETH
- zdecydowano się na hard fork, ETH złamało zasadę **nieodwracalności**
- część osób dalej wspiera starą sieć, zwaną odtąd **Ethereum Classic** (ETC)
- Ethereum tym samym straciło część zaufania

Spis treści

1 Wstęp

2 Bitcoin

3 Ethereum

4 Nie proof-of-work

5 Ataki

6 Wykresy

7 Podsumowanie

Proof-of-work

- Wykonywanie kosztownych operacji jest kosztowne
- Marnowane są pieniądze i prąd, by mieć szanse na wzbogacenie się
- Niewinne kopalnie są perfidnie eksploatowane by ludzie mogli policzyć sobie jakieś hashe
- Kopalnie kryptowalut ogrzewają Ziemię

Nasuwa się pytanie:
Czy nie można byłoby zrobić tego lepiej dla środowiska i naszych portfeli?

Proof-of-space (PoSpace), proof-of-capacity (PoC)

- zamiast obliczeń używamy **pamięć**
- małe zużycie energii
- używane w SpaceMint i Burstcoin
- trudno jest osobie udowadniającej przejście testu jeśli nie zarezerwuje odpowiedniej ilości pamięci
- przykładowa implementacja: **hard-to-pebble graphs**

Proof-of-stake

- Osoba chcąca stworzyć następny blok deponuje pewną ilość pieniędzy (stake)
- Wybieranie jest losowe i na podstawie depozytu, czasu zamrożenia pieniędzy, czy innego parametru
- Selekcja osoby tworzącej następny blok tylko za pomocą bogactwa nie ma sensu – zdecentralizowałoby to sieć.
- Np. w Peercoin-ie im dłużej coiny były nieruchome, tym większą mają siłę tworzenia nowego bloku
- Zamiast kopaczy mamy **walidatorów**
- Zamiast kopania mamy bicie pieniędzy (**mint**) lub kucie (**forge**)

Proof-of-authority (PoA)

- W PoA mamy **walidatorów**.
- Mając dobrą reputację można zostać walidatorem.
- Walidatorzy mają prawo tworzyć bloki.
- Walidator nie może stworzyć więcej niż 1 kolejny blok.
- PoA może być wykorzystywany w sieciach **prywatnych**.
- Nic nie trzeba kopać.

Spis treści

1 Wstęp

2 Bitcoin

3 Ethereum

4 Nie proof-of-work

5 Ataki

6 Wykresy

7 Podsumowanie

Atak 51%

Przedstawiony przez Satoshi Nakamoto w "bitcoin.pdf"

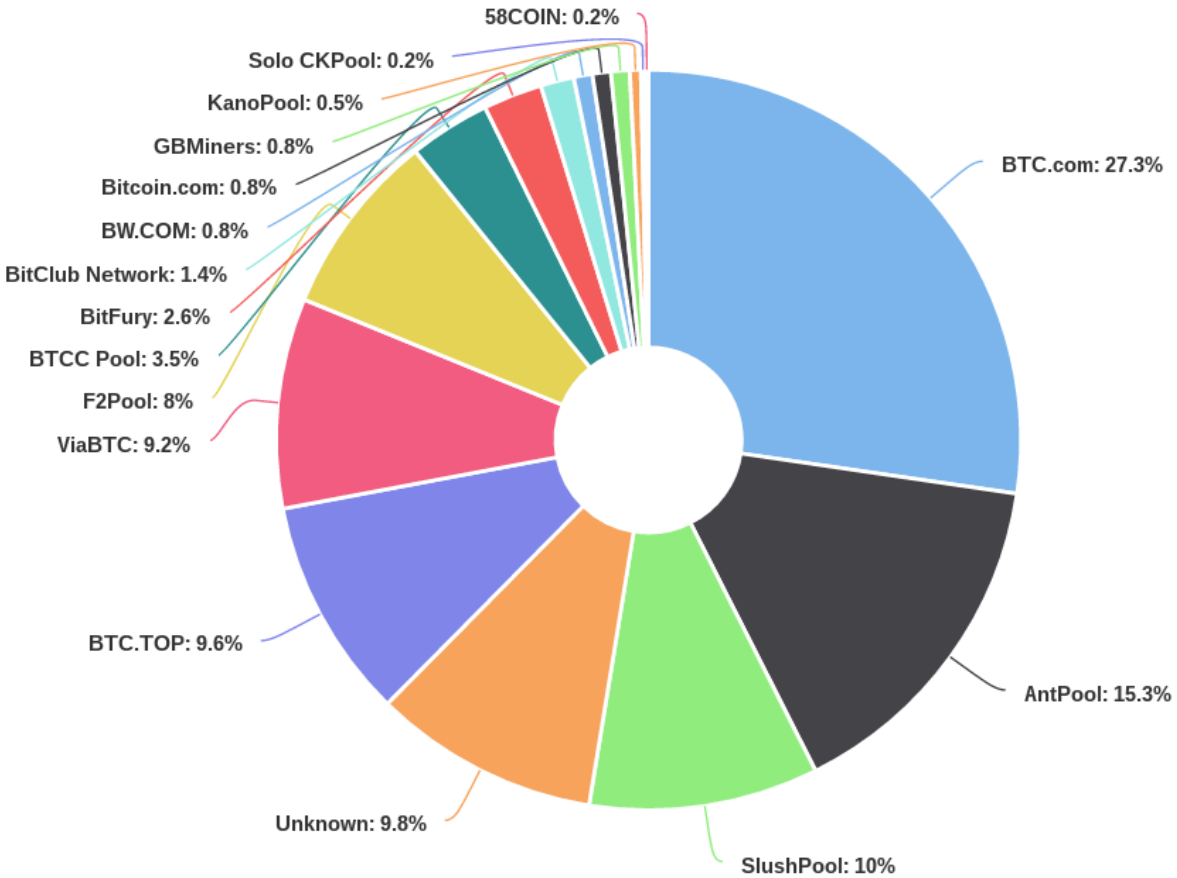
- Nieuczciwy atakujący ma większość mocy obliczeniowej sieci
- Może ignorować całkowicie bloki innych i kopać tylko swoje
- Może zablokować potwierdzanie transakcji
- Może oszukiwać ludzi, którzy nie sprawdzają całych bloków

Ciekawe zdarzenie miało miejsce w 2014 roku:

- **Pool** zwany GHash.IO zdobył ponad 51% mocy sieci
- Zrodziła się pewna panika
- Ludzie zaczęli zmieniać GHash.IO na inne poole
- GHash.IO szybko stracił "dominację" nad siecią

Atak 51% (2)

Wykres mocy pooli.
Do ataku 51% wystarczy zjednoczenie kilku pooli:



Sybil attack

- Nazwa od kobiety, która miała problem wielu osobowości
- Atakujący udaje dużo klientów sieci p2p
  Na przykład przejmując niezabezpieczone komputery
- Prawdopodobieństwo, że połączymy się z klientami atakującego jest duże

Możliwe sposoby wykorzystania:

- Atakujący nie przyjmuje nowych bloków – jesteśmy odcięci od sieci
- Atakujący przyjmuje tylko bloki wykopane przez siebie – jesteśmy w oddzielnej (wolniejszej) sieci

Atak DoS (Denial of Service)

Atakujący wysyła dużo danych do węzła sieci. Węzeł **nie ma czasu** sprawdzać normalnych transakcji/bloków.

Mechanizmy obrony:

- Węzły nie przekazują osieroconych i niepoprawnych transakcji/bloków
- Węzły banują źle zachowujące się IP adresy na 24h
- Wielkość bloku nie może przekroczyć pewnej wielkości, np. 1MB
- Inne limity na wielkości, np. skryptów

Ataki kryptograficzne

- Złamanie funkcji hashującej (np. SHA256) – mało prawdopodobne. Sieć może przenieść się na inną funkcję hashującą.
- Generowanie wielu adresów – strata czasu.
  W Bitcoinie klucz ma 256bitów, hashuje się do 160bitowego adresu. Wychodzi około $2.15x10^{38}$ adresów na osobę.
- Ale kiedyś Androidowy generator liczb losowych był słaby i generowanie adresów na Androidzie rzeczywiście miało sens.

Spis treści

1 Wstęp

2 Bitcoin

3 Ethereum

4 Nie proof-of-work

5 Ataki

6 Wykresy

7 Podsumowanie

Wykresy?

Być może warto pokazać kilka wykresów dotyczących blockchaina w Bitcoinie.

O ile jest jeszcze trochę czasu

Spis treści

1 Wstęp

2 Bitcoin

3 Ethereum

4 Nie proof-of-work

5 Ataki

6 Wykresy

7 Podsumowanie

Podsumowanie

- Blockchain został stworzony do uzgadniania wspólnej spójnej historii/rejestru dla całej sieci
- Jest on raczej ideą tworzenia bezpiecznych łańcuchów bloków niż konkretną implementacją
- Blockchain może wykorzystywać różne mechanizmy uzgadniania kolejnego bloku
- Transakcje umieszczone w bloku są niemal niemożliwe do odwrócenia

Źródła (1)

Dobre źródła informacji:

- bitcoin.org
  Bitcoin paper: https://bitcoin.org/bitcoin.pdf
  Dużo szczegółów technicznych: https://bitcoin.org/en/developer-guide
- Bitcoin wiki: https://en.bitcoin.it/
  https://en.bitcoin.it/wiki/Difficulty
- Wykresy: https://charts.bitcoin.com/
- Giełda/ceny kryptowalut: https://bitbay.net/pl/kurs-walut
- Bitcoin blockchain: https://blockchain.info/
- Wikipedia, Blockchain: https://en.wikipedia.org/wiki/Blockchain

Źródła (2)

Forki:

- Przekręcenie licznika w Bitcoinie: https://en.bitcoin.it/wiki/Value_overflow_incident
- Ethereum: http://bitcoin.pl/wiadomosci/ciekawostki/1261-ethereum-po-hard-forku-kolejna-lekcja-dla-swiata-kryptowalut https://www.quora.com/Why-did-Ethereum-and-Ethereum-Classic-split

Bezpieczeństwo:

- Ogólne słabości: https://en.bitcoin.it/wiki/Weaknesses
- Ataki na sieć: http://resources.infosecinstitute.com/blockchain-networks-possible-attacks-ways-protection/
- 51% Pool: www.economist.com/blogs/schumpeter/2014/06/bitcoin
- Androidowy bug: https://www.digitaltrends.com/mobile/how-to-fix-bitcoin-android-bug/

Koniec

Pytania?

Dziękuję za uwagę