Blockchain okiem fizyka

P. F. Góra

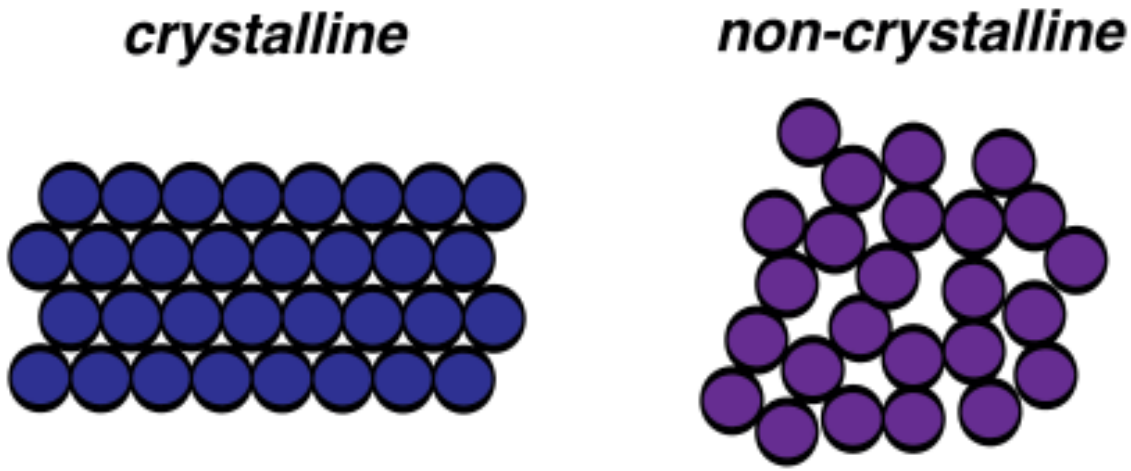
Wydział Fizyki, Astronomii i Informatyki Stosowanej UJ
Komisja Układów Złożonych PAU
http://th-www.if.uj.edu.pl/zfs/gora/

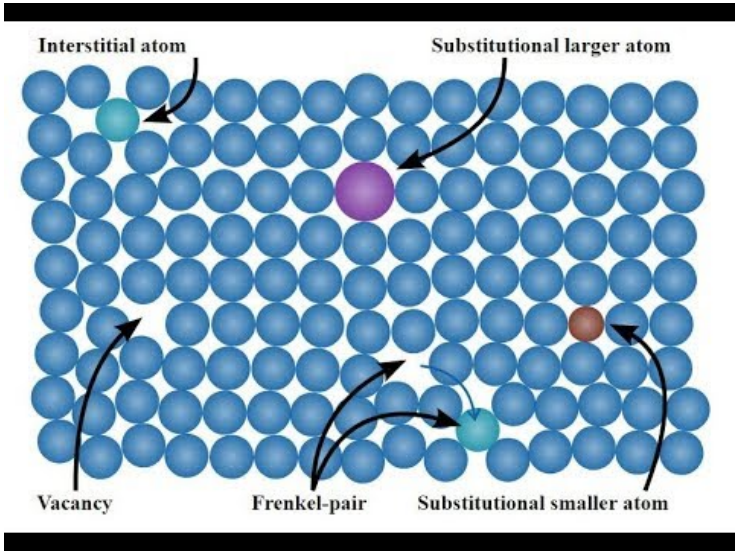
13 listopada 2020

Streszczenie

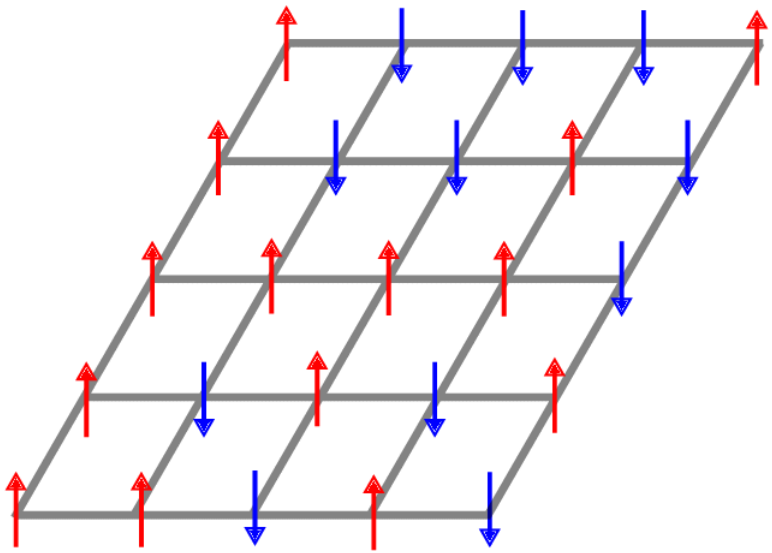
Blockchain to specjalistyczna, zdecentralizowana baza danych, działająca w sieci P2P.
Dlaczego fizycy zajmują się sieciami komputerowymi? Albo bazami danych? Czy mają coś nowego do powiedzenia?

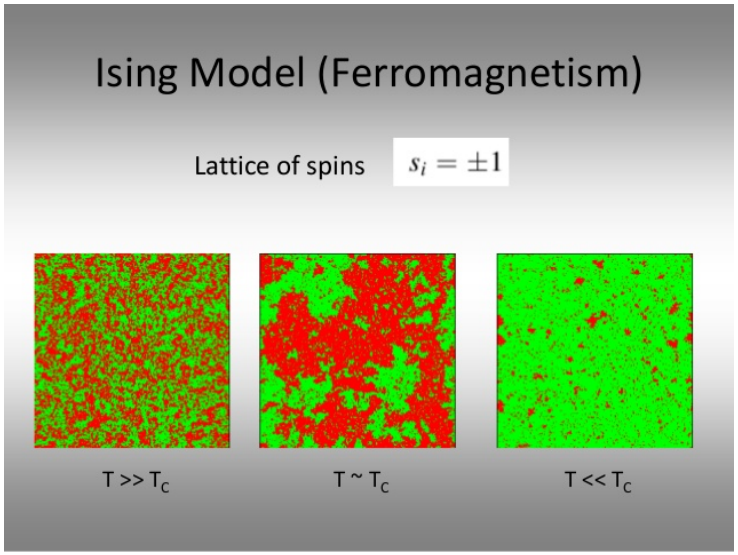
Sieć krystaliczna



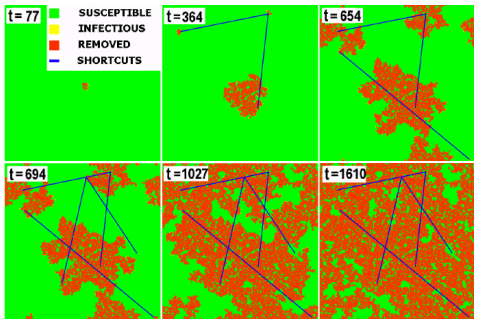


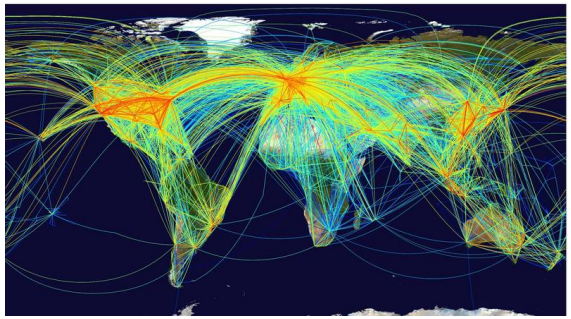
Model Isinga

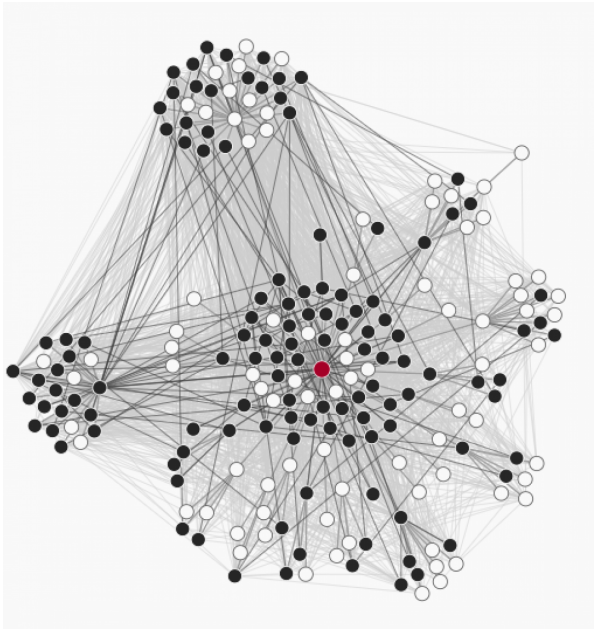




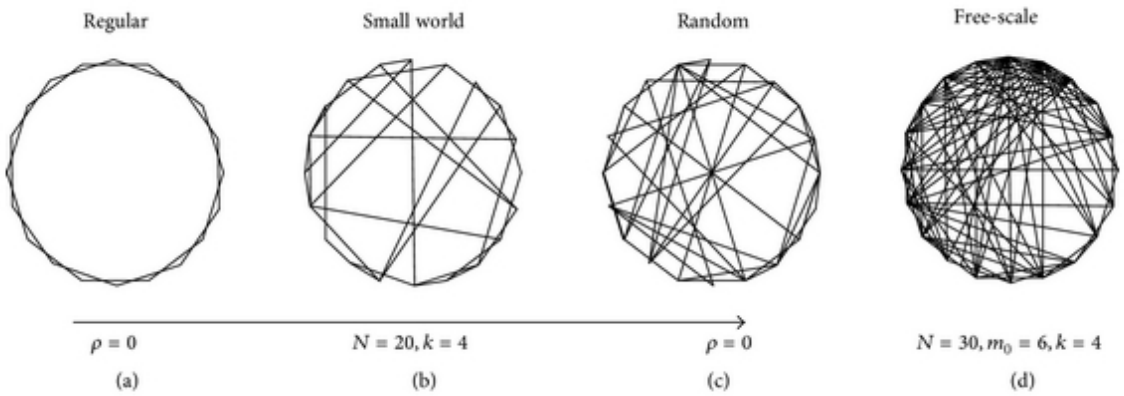
Epidemie

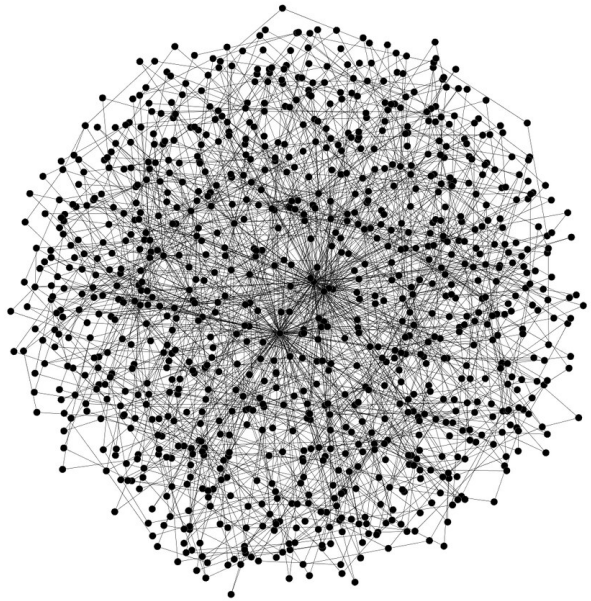

t = 77
SUSCEPTIBLE
INFECTIOUS
REMOVED
SHORTCUTS
t = 364
t = 654
t = 694
t = 1027
t = 1610



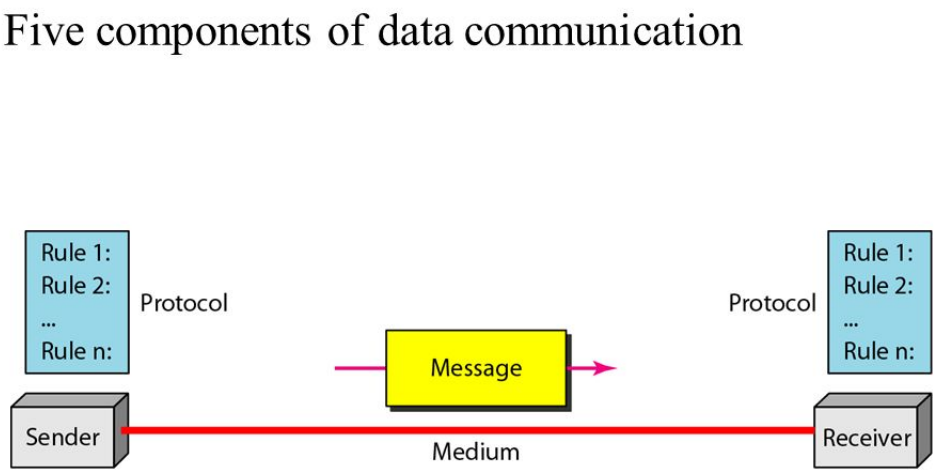


Ewoluujące sieci





Wymiana informacji jako oddziaływanie



Komputery w sieci porozumiewają się wymieniając komunikaty. Wymiana komunikatu oznacza wymianę informacji.

Dla fizyków wymiana informacji oznacza **oddziaływanie**.

“Hamiltonian” wymiany informacji

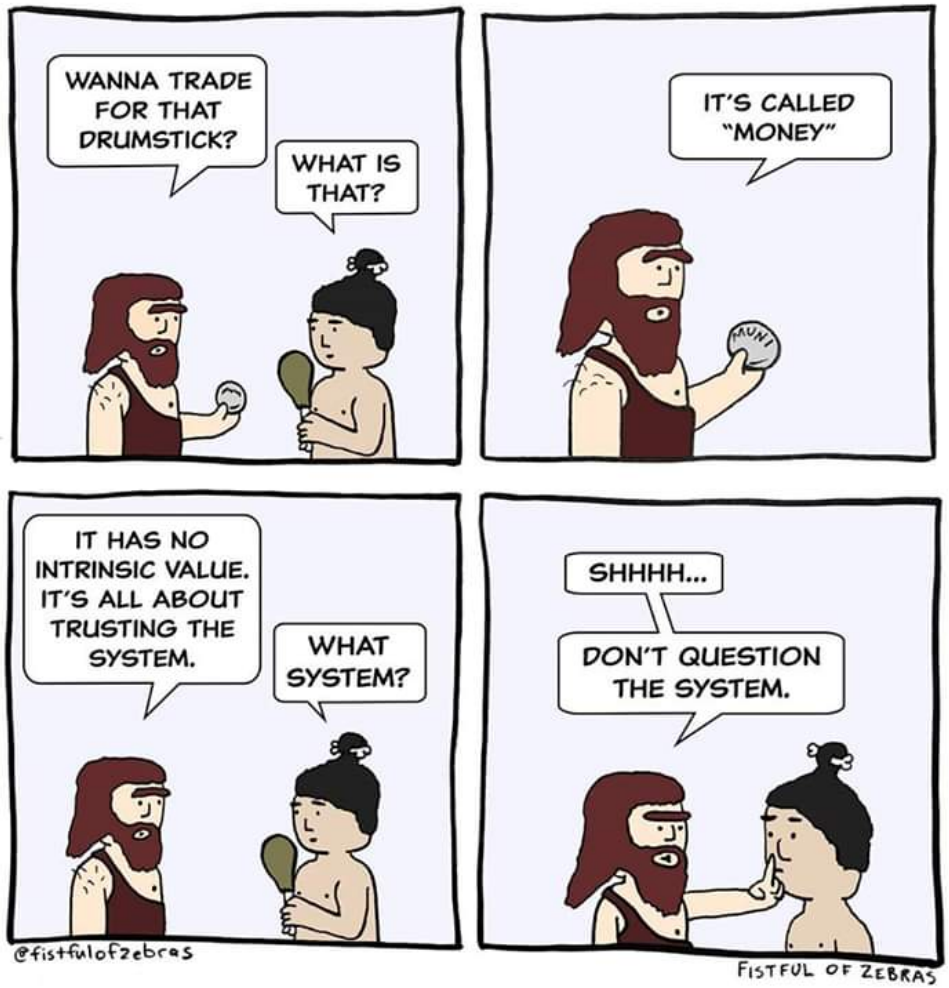
Dana jest pewna sieć. Stan sieci zmienia się synchronicznie, co ustalony krok czasowy Δt. Stan i-tego węzła w chwili n (tzn. $0 + n \cdot \Delta t$) opisuje wielkość f_i. Proces oddziaływania poprzez wymianę informacji możemy **w przybliżeniu** opisać jako

$$f_i(n+1) = \sum_j P_{ij}(n)\, \mathcal{F}(f_i, f_j)\,.$$

$P_{ij}(n)$ to zależna od czasu macierz połączeń

$$P_{ij}(n) = \begin{cases} 1 & \text{komunikat od } j \text{ do i w interwale } [n\Delta t, (n+1)\Delta t] \\ 0 & \text{brak takiego komunikatu} \end{cases}$$

Cała “fizyka” tkwi w funkcji $\mathcal{F}(f_i, f_j)$.


WANNA TRADE FOR THAT DRUMSTICK?
WHAT IS THAT?
IT'S CALLED "MONEY"
MUNI
IT HAS NO INTRINSIC VALUE. IT'S ALL ABOUT TRUSTING THE SYSTEM.
WHAT SYSTEM?
SHHHH...
DON'T QUESTION THE SYSTEM.
@fistfulofzebras
FISTFUL OF ZEBRAS

Blockchain — motywacja

Dwa problemy z pieniądzem fiducjarnym:

1. Double-spending: jak zapewnić, że **te same** pieniądze nie zostaną wydane dwukrotnie?
2. Zaufana trzecia strona: Czy naprawdę możemy (i chcemy) zaufać, oddając przy okazji część kontroli?

Blockchain — historia

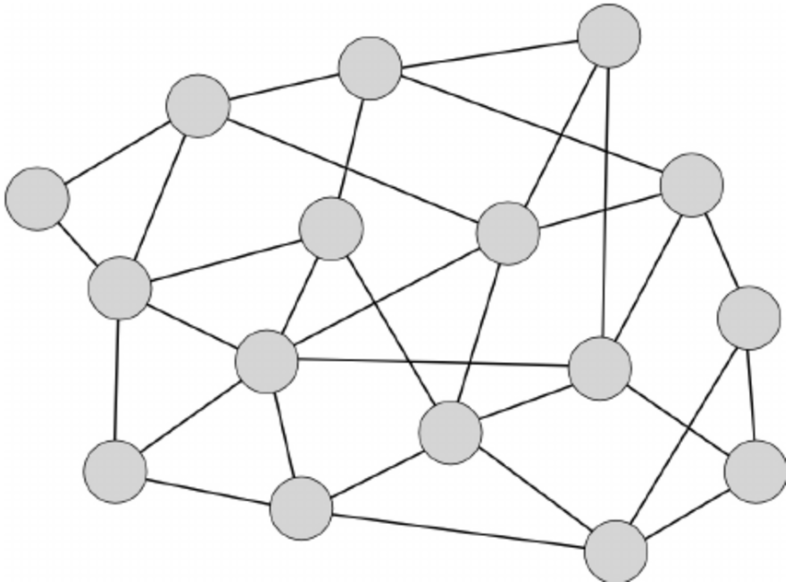
Blockchain i pierwsza kryptowaluta, Bitcoin, zostały zaproponowane w 2008 przez Satoshi Nakamoto. Zostały wprowadzone w życie w 2009.
Nikt nie wie, kim jest Satoshi Nakamoto ☺
Oryginalny artykuł Satoshi Nakamoto można przeczytać tutaj.

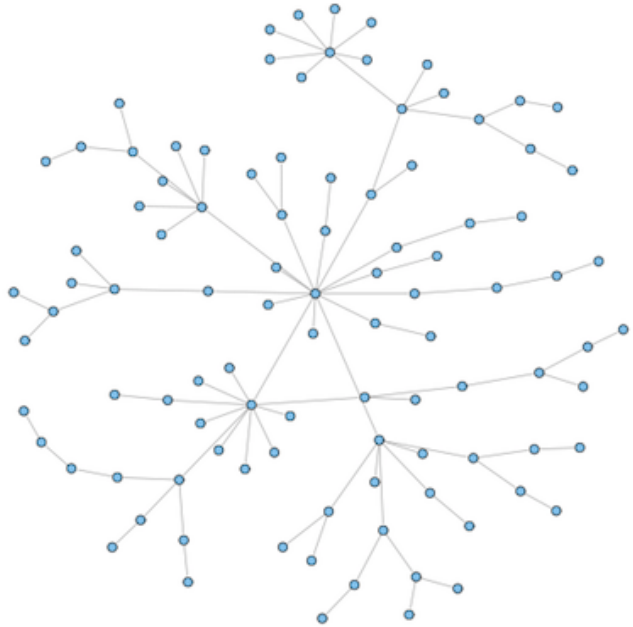
Abstract

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Z punktu widzenia baz danych…

Blockchain jest specjalistyczną, rozproszoną, zdecentralizowaną, nietransakcyjną bazą danych w modelu peer-to-peer (P2P). Blockchain to publiczny i jawny rejestr "transakcji" lub "operacji księgowych" (*public ledger*), zapewniający bezpieczeństwo i niezmienność raz zapisanych operacji na drodze kryptograficznej.





W sieci P2P komputery są połączone i mogą współdzielić zasoby bez konieczności odwoływania się do zewnętrznego serwera.
Po lewej — idealna sieć P2P. Po prawej — sieć bezskalowa, w której widoczne centra (*hubs*) wyróżniają się ze względu na liczbę połączeń, ale nie ze względu na *formalną* rolę, jaką pełnią w sieci.

Elementy blockchain

Transakcje oznaczają elementarne operacje obsługiwane przez dany blockchain. *Transakcją* może być wymiana jakichś tokenów — na przykład kryptowalut — w zamian za pewne inne dobra lub usługi, ale gdzie indziej transakcją może być zapisanie jakiegoś pliku, zrealizowanie inteligentnego kontraktu (*smart contract*), potwierdzenie operacji, która miała miejsce w świecie rzeczywistym, dokonanie zmian w pewnym rejestrze itp. Każda transakcja podpisywana jest za pomocą klucza publicznego. Transakcje są jawne, choć użytkownicy mogą pozostawać anonimowi. Węzły dokonujące transakcji informują o jej dokonaniu wszystkie węzły, z którymi są połączone. Każda poprawna transakcja zapisywana jest w buforze transakcji. Obsługa transakcji na ogół nie jest darmowa.

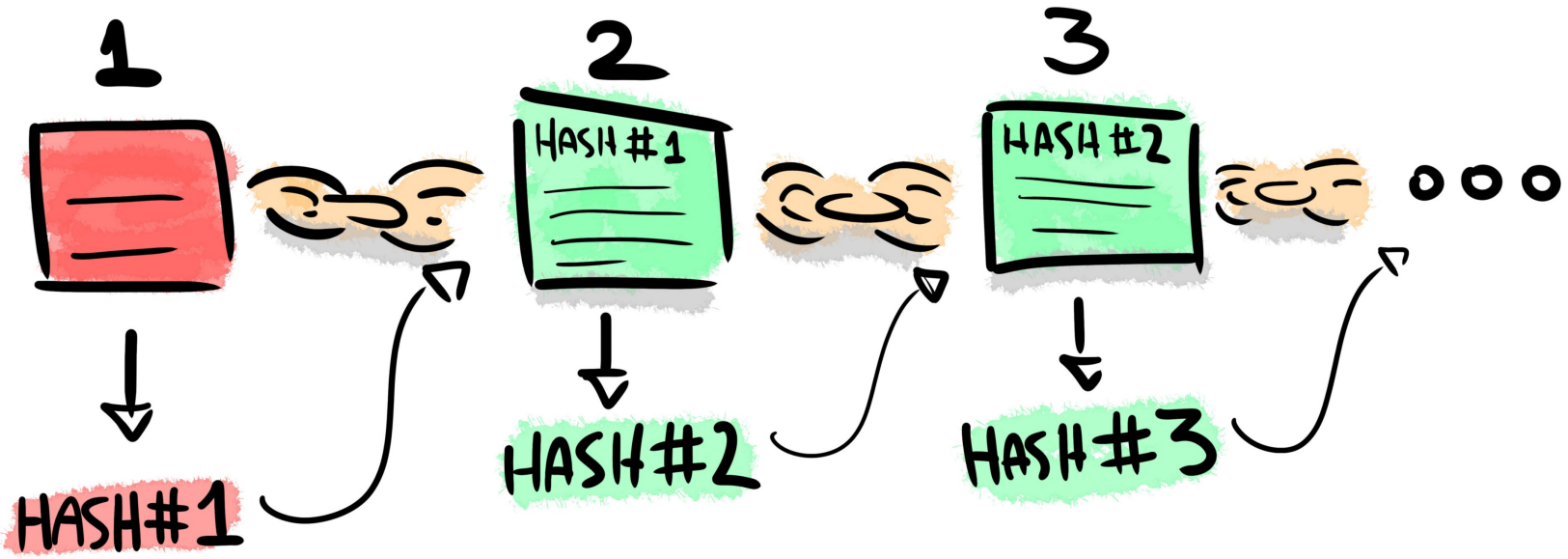
Blok zawiera określoną liczbę transkacji **oraz hash** poprzedniego bloku, co w chwili tworzenia oznacza ostatni, najmłodszy blok z blockchain, a także *nonce*, czterobajtową, unikalną liczbę, której wartość ustala się w procesie zatwierdzania bloku.

Zatwierdzenie bloku oparte jest na rozwiązaniu pewnego problemu kryptograficznego. Węzeł zatwierdzający blok pobiera transakcje z bufora, tworzy nowy blok i próbuje rozwiązać problem kryptograficzny. W sieci Bitcoin jedynym znanym sposobem jest rozwiązanie siłowe, stąd wymaga to dużych (właściwie należałoby powiedzieć: **bardzo dużych**) mocy obliczeniowych. Jest to tak zwany *Proof of Work* (PoW). (Możliwe są także inne sposoby zatwierdzania nowych bloków, takie jak *Proof of Stake*. PoS nie wymaga tak potężnych mocy obliczeniowych, jak PoW. Niektóre “alternatywne” kryptowaluty oparte są o PoS.) Po rozwiązaniu problemu, węzeł, który tego dokonał, dołącza ten blok do swojej kopii blockchain i rozsyła ten blockchain do pozostałych węzłów sieci.

Górnicy (kopacze, *miners*) to wyspecjalizowane węzły zajmujące się zatwierdzaniem bloków. Specjalizacja jest potrzebna z uwagi na wymaganie posiadania wielkich mocy obliczeniowych. Górnicy mogą (chociaż nie muszą) otrzymywać wynagrodzenie za skuteczne zatwierdzenie każdego bloku.

Dołączanie nowego bloku Każdy węzeł przechowuje swoją kopię całego rejestru (czyli łańcucha bloków, czyli blockchain). Węzeł, który otrzyma nowy łańcuch, po pierwsze sprawdza, czy najnowszy blok został utworzony poprawnie (sprawdzenie, w przeciwieństwie do samego dołączenia, jest łatwe i tanie), a następnie z dwu posiadanych egzemplarzy blockchain (dotychczasowy i nowootrzymany) wybiera dłuższy. Zatwierdzanie bloków przez górników, weryfikacja przez pozostałe węzły i zasada utrzymywania najdłuższego łańcucha stanowią mechanizm osiągania konsensusu w sieci blockchain.

Bloki osierocone (*orphaned block*). Może się zdarzyć, że na skutek opóźnień czasowych lub partycjonowania sieci blockchain zbifurkuje, rozszczepi się. Wówczas węzły będą akceptować dłuższą gałąź. Bloki z krótszej gałęzi zostają “osierocone”. Są to poprawnie zweryfikowane bloki, ale ponieważ nie mogą zostać dołączone do blockchain, zawarte w nich transakcje wracają do bufora transakcji.



Ponieważ hasz całego bloku zależy od zawartości bloku **oraz** od hasza do jego poprzednika, nie da się zmienić bloku (czyli sfałszować lub usunąć już zatwierdzonych transakcji) bez konieczności ponownego zatwierdzenia wszystkich następnych bloków w łańcuchu, co jest praktycznie niewykonalne w szybkim czasie z uwagi na monstrualną moc obliczeniową potrzebną do wykonania takiego zadania.

Bitcoin: wynagrodzenie górników

W sieci Bitcoin górnicy za zatwierdzenie każdego bloku otrzymują wynagrodzenie: kreowane są **nowe** bitcoiny, które otrzymuje górnik zatwierdzający nowy blok. Ponieważ z założenia nie może być więcej, niż 21 mln ₿, nagroda za zatwierdzenie bloku zmniejsza się o połowę po każdych zatwierdzonych 210 000 blokach. Jeden blok zatwierdzany jest co około 10 minut.

- W 2009 nagroda za wygenerowanie bloku wynosiła 50₿.
- Od 2012 nagroda wynosiła 25₿.
- Od 2016 nagroda wynosi 12.5₿.
- 12 maja 2020 nagroda spadł do 6.25₿. Jej wartość w "normalnym" pieniądzu wynosi obecnie około 100 000 USD.
- Będzie jeszcze jedno obniżenie nagrody.
- Po wygenerowaniu **wszystkich możliwych bitcoinów**, nowe bitcoiny przestaną być generowane, a górnicy będą wynagradzani z drobnych opłat transakcyjnych.

Aktualny stan tego procesu można śledzić na stronie `https://www.bitcoinblockhalf.com/` (warto ją co kilka minut odświeżyć).

1 ₿ jest obecnie wart około $16000 (w grudniu 2017 bitcoin osiągnął swój najwyższy kurs $19035.60). Gdy wygłaszałem ten wykład niecały rok temu, kurs bitcoina wynosił około $8300 — zmiennośc kursu (*volatility*) jest **bardzo** duża.

Wydobywanie bitcoinów, które miało być rodzajem *community service*, z uwagi na swoją opłacalność stało się celem samym w sobie. Szacuje się, że obecnie około 60% bitcoinów w obiegu znajduje się w posiadaniu górników.

Szacuje się, że Satoshi Nakamoto — kimkolwiek jest — posiada pomiędzy 200 000 a 600 000₿.

Co robią fizycy?

- Kopią bitcoiny? Niektórzy być może tak…
  Ale nie w ramach działalności zawodowej.

Co robią fizycy?

- Kopią bitcoiny? Niektórzy być może tak…
  Ale nie w ramach działalności zawodowej.
- Modelują i analizują proces generowania bitcoinów?

Co robią fizycy?

- Kopią bitcoiny? Niektórzy być może tak…
  Ale nie w ramach działalności zawodowej.
- Modelują i analizują proces generowania bitcoinów? Tak! ☺

Dotychczasowe rezultaty

- Współistnieją dwie sprzężone, oddziałujące sieci: sieć P2P i sieć transakcji ekonomicznych.
- Bloki zatwierdzane są w procesie Poissona (pewnym procesie stochastycznym).
- Analizowane problemy: Topologia sieci, rozkład zdolności do kopania bitcoinów, liczba węzłów, zależnośc od czasu propagacji, czas osiągania konsensusu.
- Główny wniosek: Zachowanie sieci (czas osiągania konsensusu) *słabo* zależy od topologii sieci.
- Jak zachowanie sieci zależy od
  - rozkładu zdolności do kopania bitcoinów (jeśli rozkład jest długoogonowy)...?
  - dynamiki **ewoluującej** sieci: "słabe" węzły są odłączane, nowe są dołączane w procesie bezskalowym?
  - jak na ten proces wypłynie spadek nagrody za zatwierdzenie bloku?

W jaki sposób kryptowaluty oparte o blockchain rozwiązują problem “double spending”?

promocja.fais@uj.edu.pl