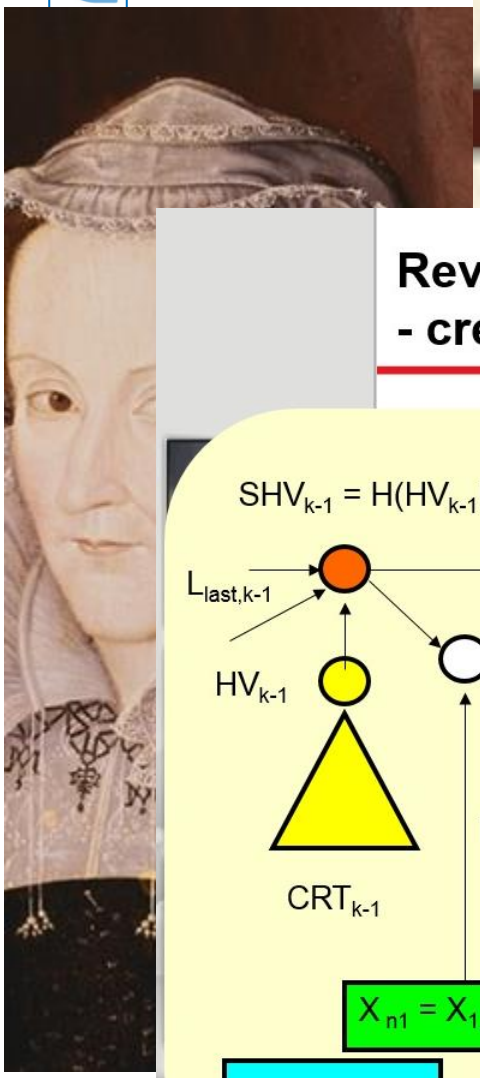
Część 7

Kryptograficzne podstawy technologii blockchain


POLAND
DOING BLOCKCHAIN SINCE 1966



RSA Conference 2002

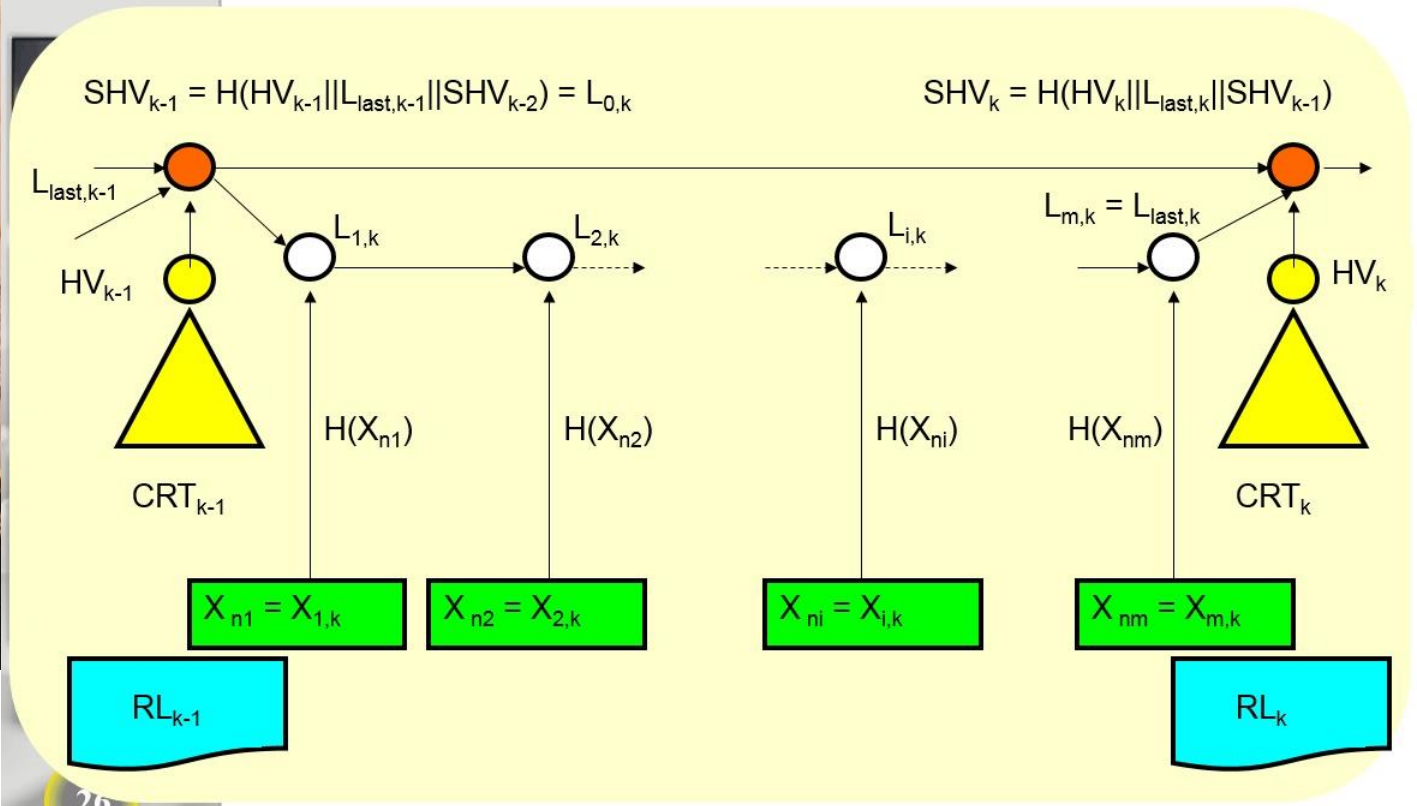
Theme Tracks Microsoft Sponsors Exhibitors Search

DAY 16:15

iversity of

verification
and cons of
on Trees
ysis is the
Trees (LCRT)

Revoked Certificates Data Base (RCDB) Structure - creation diagram



Plan wykładu

1. **Wstęp, co to jest Blockchain?**
2. **Bitcoin**
3. **Bitcoin w praktyce**
4. **Blockchain a wymagania bezpieczeństwa**
5. **Podsumowanie**

Plan wykładu

1. **Wstęp, co to jest Blockchain?**
2. **Bitcoin**
3. **Bitcoin w praktyce**
4. **Blockchain a wymagania bezpieczeństwa**
5. **Podsumowanie**

Blockchain vs Bitcoin

- **Blockchain (łańcuch bloków):**
  - **prywatny – dostępny wyłącznie dla autoryzowanych podmiotów**
  - **publiczny – dostępny dla każdego**
- **Dane w Blockchain przechowuje się na dwa sposoby:**
  - **On-chain storage – wszystkie dane przechowuje się w blockchain**
  - **Off-chain storage – w blockchain przechowuje się wybrane dane (np. tylko skróty)**
- **Bitcoin to kryptowaluta wykorzystująca jeden z typów blockchain: publiczny z *on-chain storage***

Czym jest blockchain? 1/2

Problem:

Jak zapewnić integralność grupy dokumentów/transakcji?

- **musi być zachowana kolejność dodania dokumentów**
- **nie może być możliwe antydatowanie**
- **możliwe jest wykrywanie brakujących dokumentów**

Rozwiązanie tradycyjne (bez blockchain):

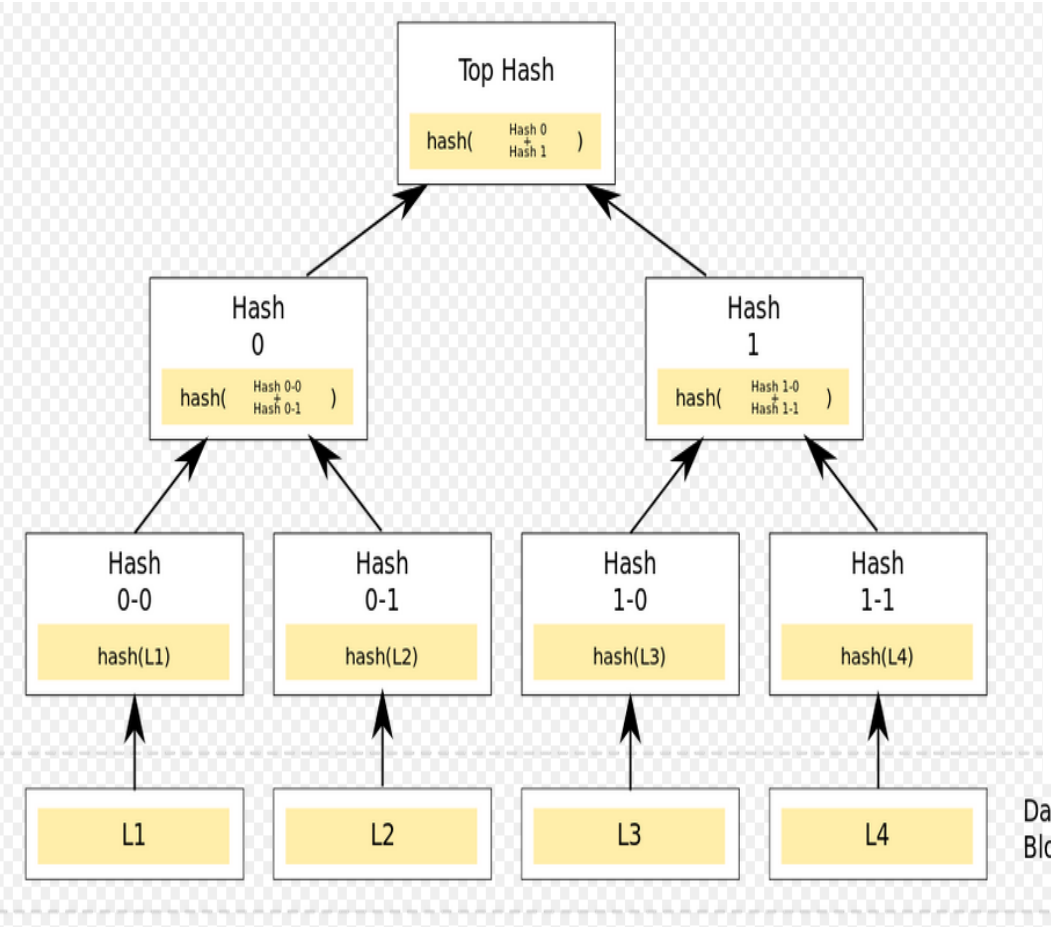
Znane od lat 90-tych ubiegłego stulecia.

Wykorzystanie:

- **liniowego łączenia skrótów lub drzewa Merkla**
- **znacznika czasu od zaufanych urzędów certyfikacji (CA) - znaczniki czasu zabezpieczają przed modyfikacją wstecz łańcucha skrótów**

Drzewo Merkle'a

1979



Umożliwia powiązanie krypto-graficzne informacji o blokach danych w celu kontroli ich integralności /autentyczności. Zazwyczaj autentyczność wartości skrótu skojarzonego z korzeniem drzewa (root hash/top hash) zapewniana jest dzięki weryfikacji podpisu „zaufanego podmiotu" złożonego tylko na tej wartości. Weryfikacja autentyczności i integralności dowolnego bloku danych skojarzonego z liściem drzewa wymaga (po weryfikacji podpisu „na korzeniu") sprawdzenia tylko integralności ścieżki złożonej z węzłów rodzicielskich dla wskazanego bloku danych (złożoność logarytmiczna!), bez znajomości innych bloków danych.

Źródło rysunku: http;//en.wikipedia.org/wiki/Merkle_tree

Czym jest blockchain? 2/2

Główne wady stosowania zaufanych znaczników czasu:

- **centralizacja – jak ustalić wspólną wersję łańcucha bloków, gdy wiele podmiotów musi dodawać bloki (lub tylko skróty) do łańcucha bloków? Wyznacza się jeden lub kilka serwerów (centralizacja), które będą ustalały wspólną wersję**

Blok to wiele połączonych skrótów np. za pomocą drzewa Merkla, może zawierać dokumenty/transakcje, z których policzono skróty

Pożądane cechy:

- **decentralizacja**
- **brak konieczności zaufania konkretnym usługom**
- **skalowalność dla wielu podmiotów**

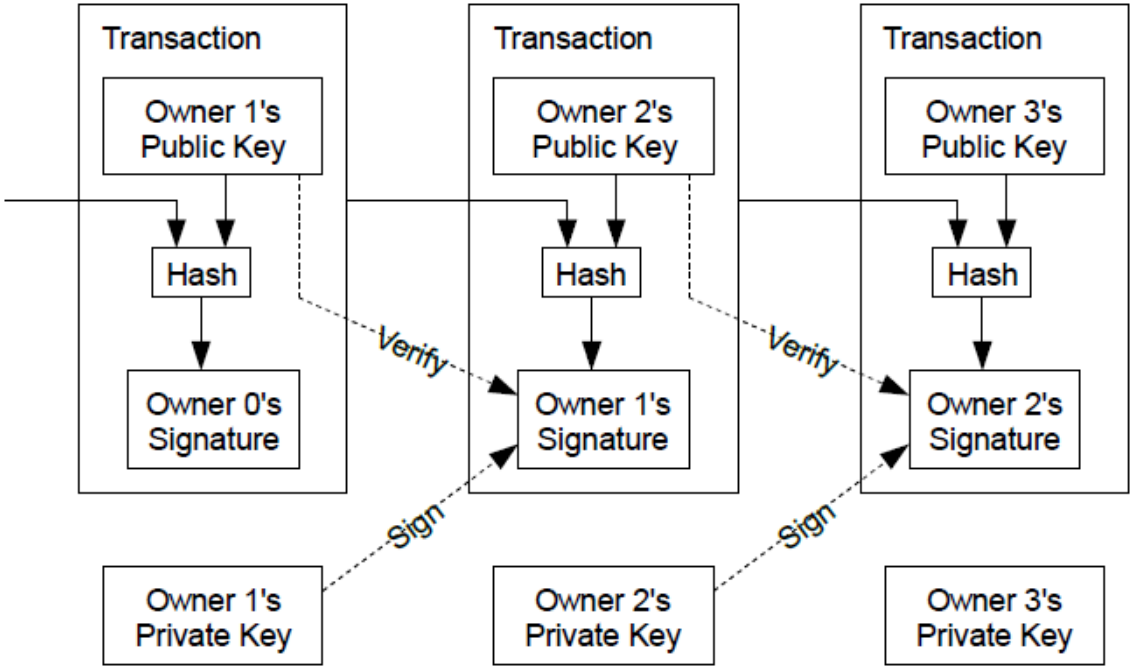
Blockchain = mechanizm wiązania bloków + protokół konsensusu

Plan wykładu

1. Wstęp, co to jest Blockchain?
2. **Bitcoin**
3. Bitcoin w praktyce
4. Blockchain a wymagania bezpieczeństwa
5. Podsumowanie

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto - 2008



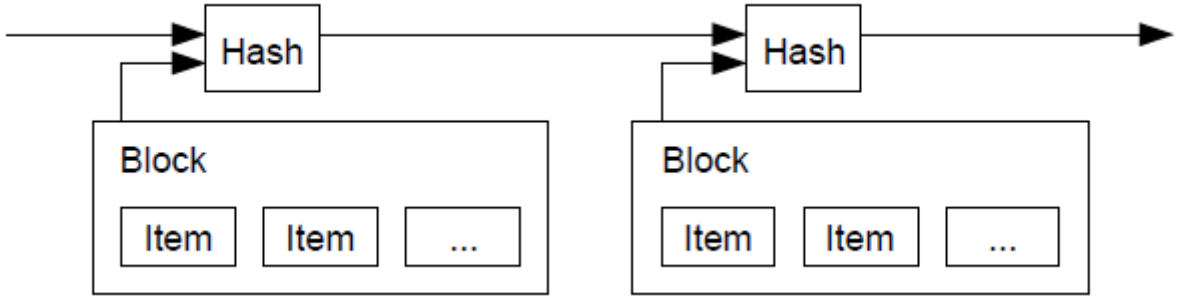
Umożliwia płatności w sieci peer-to-peer. Płatność jest podpisywana kluczem prywatnym płatnika, zaś jego klucz publiczny pełni rolę „identyfikatora ostatniej transakcji” w łańcuchu kolejnych płatności powiązanych funkcją skrótu.

Problem: jak uniemożliwić dwukrotne wydanie tej samej monety bez konieczności angażowania zaufanej trzeciej strony.

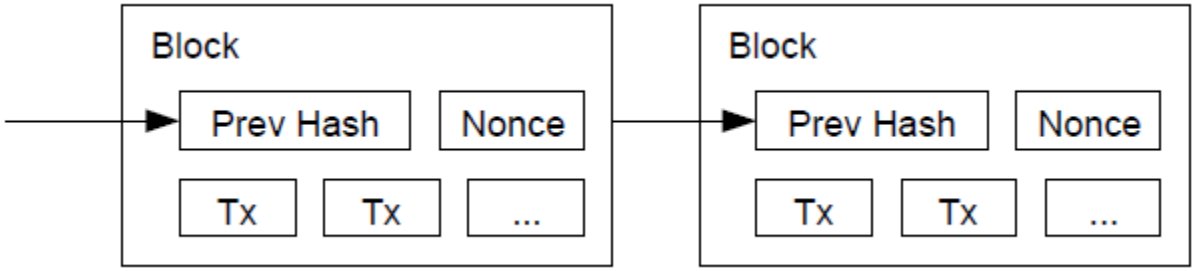
Bitcoin: A Peer-to-Peer Electronic Cash System (cd.)

- **Transakcje są skonstruowane w taki sposób, że w praktyce trudne obliczeniowo jest ich odwrócenie i wprowadzenie fałszywych transakcji.**
- **System jest bezpieczny dopóki uczciwe węzły kontrolują łącznie więcej mocy CPU niż jakakolwiek grupa współpracujących węzłów (51% uczciwych).**
- **BitCoin jest systemem elektronicznych płatności bazującym na dowodach kryptograficznych zamiast na zaufaniu, pozwalającym dwóm stronom na zawarcie transakcji bez konieczności istnienia zaufanej trzeciej strony.**
- **Wykorzystuje mechanizm Proof-of-Work (PoW) jako protokół konsensusu.**

Bitcoin: A Peer-to-Peer Electronic Cash System (cd.)



Wartości funkcji skrótu wiążącej bloki danych zawierających informację o kolejnych „losach" monety, począwszy od jej wygenerowania, opatrzone znacznikiem czasu, są publicznie dostępne.



Wartości funkcji skrótu muszą mieć określoną liczbę „zer wiodących", co jest dowodem poprawności (Proof of Work - PoW). Osiąga się to zwiększając stopniowo o 1 wartość obiektu „Nonce" podczas generowania kolejnej wartości funkcji skrótu na podstawie poprzedniej wartości (Prev Hash).

Bitcoin: A Peer-to-Peer Electronic Cash System (cd.)

Sieć działa według następującego scenariusza:

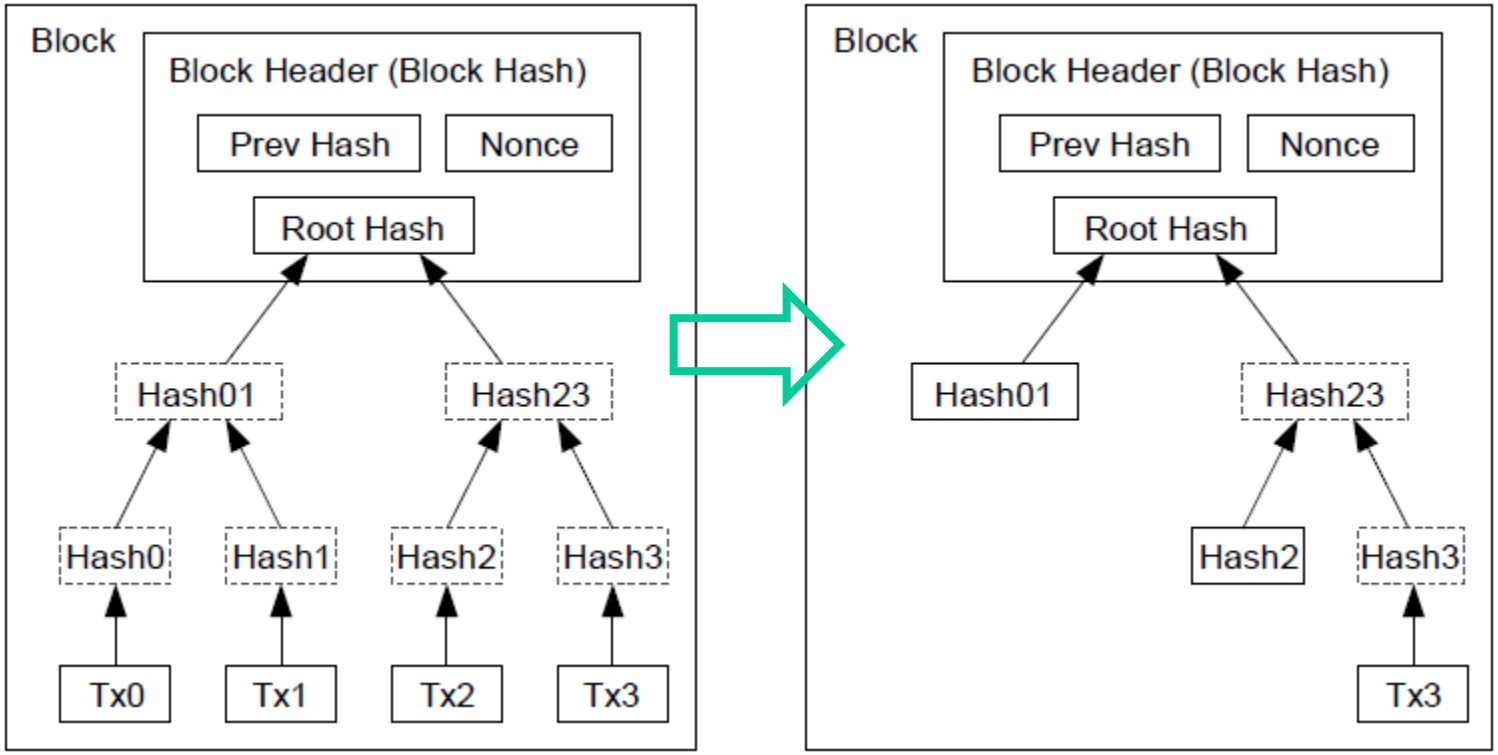
1) **Nowe transakcje są przesyłane do wszystkich węzłów sieci (broadcast).**
2) **Każdy węzeł zbiera nowe transakcje i tworzy z nich blok.**
3) **Każdy węzeł tworzy PoW dla swojego bloku (co wymaga wielokrotnych obliczeń).**
4) **Po utworzeniu PoW węzeł przesyła blok do wszystkich pozostałych węzłów.**
5) **Węzły akceptują blok wyłącznie wtedy, gdy wszystkie jego transakcje (płatności za pomocą bitcoins) są ważne i nie zostały już (ponownie) wydane.**
6) **Węzły po zaakceptowaniu bloku przystępują do tworzenia nowego bloku wykorzystując wartość skrótu zaakceptowanego bloku jako poprzedni skrót (Prev Hash).**

Węzły zawsze uznają najdłuższy łańcuch jako poprawny i wykonują działania (PoW) w celu jego wydłużenia. Jest to tzw. proces „kopania" (mining), gdyż „zwycięzca wyścigu kopaczy" – twórca nowego bloku - nagradzany jest premią (obecnie 12,5 BTC).

Jeśli dwa węzły rozsyłają jednocześnie różne wersje następnego bloku, to jeden z nich jest odbierany jako pierwszy i traktowany jako właściwy, ale drugi nie jest odrzucany, lecz zapamiętywany, gdyż może się okazać , że odpowiada dłuższemu łańcuchowi, i wtedy nastąpi „przełączenie" na ten dłuższy (ale może to prowadzić do niekorzystnego „rozwidlania łańcucha" – tzw . forking'u).

Bitcoin: A Peer-to-Peer Electronic Cash System (cd.)

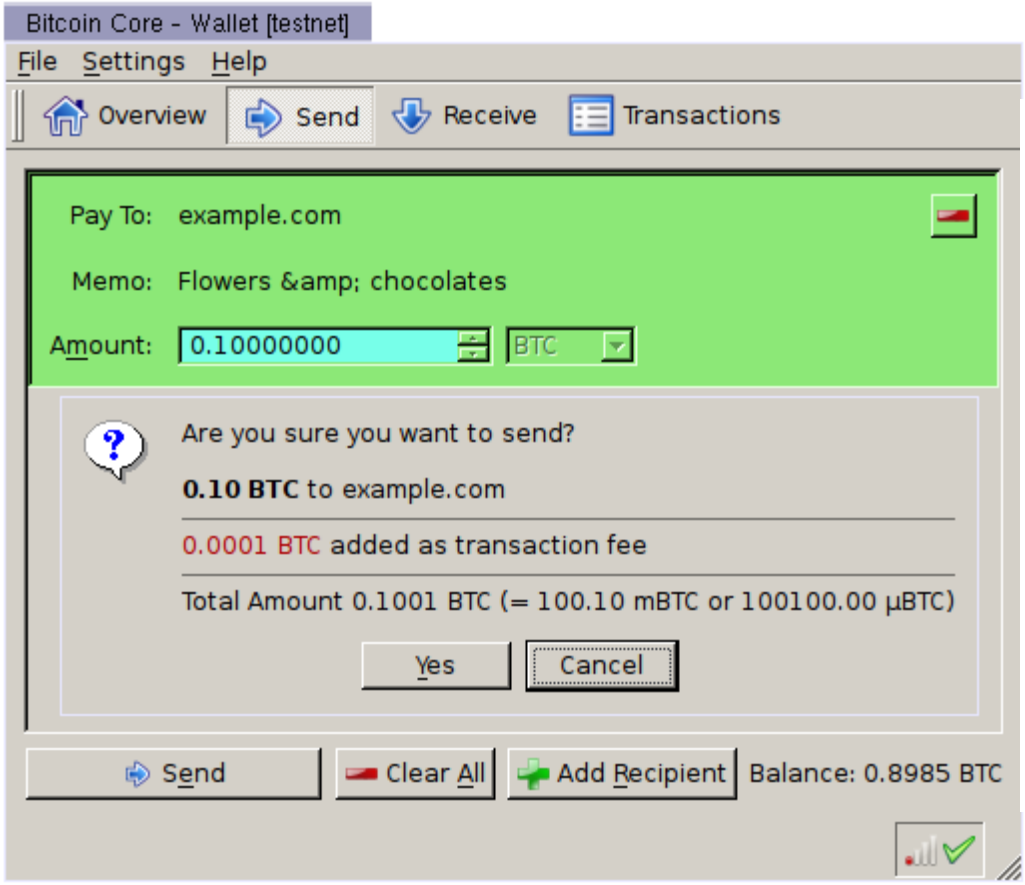
W celu uniknięcia konieczności przechowywania informacji o wszystkich poprzednich transakcjach wykonanych w łańcuchu wykorzystuje się drzewo Merkle'a.



Nagłówek (Block Header) bez transakcji zajmowałby około 80 bajtów.
Jeżeli założyć, że bloki będą generowane co 10 minut, to w ciągu roku pamięć niezbędna do przechowywania bloku wynosiłaby 80 bytes * 6 * 24 * 365 = 4.2MB.

Bitcoin: A Peer-to-Peer Electronic Cash System (cd.)

Monety przechowywane są w portfelu klienta.



Wykorzystywane algorytmy:

Elliptic Curve Digital Signature Algorithm (ECDSA) z krzywą secp256k1 ;

klucze prywatne to 256-bitowe dane generowane losowo z zakresu od 0x01 do 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140.

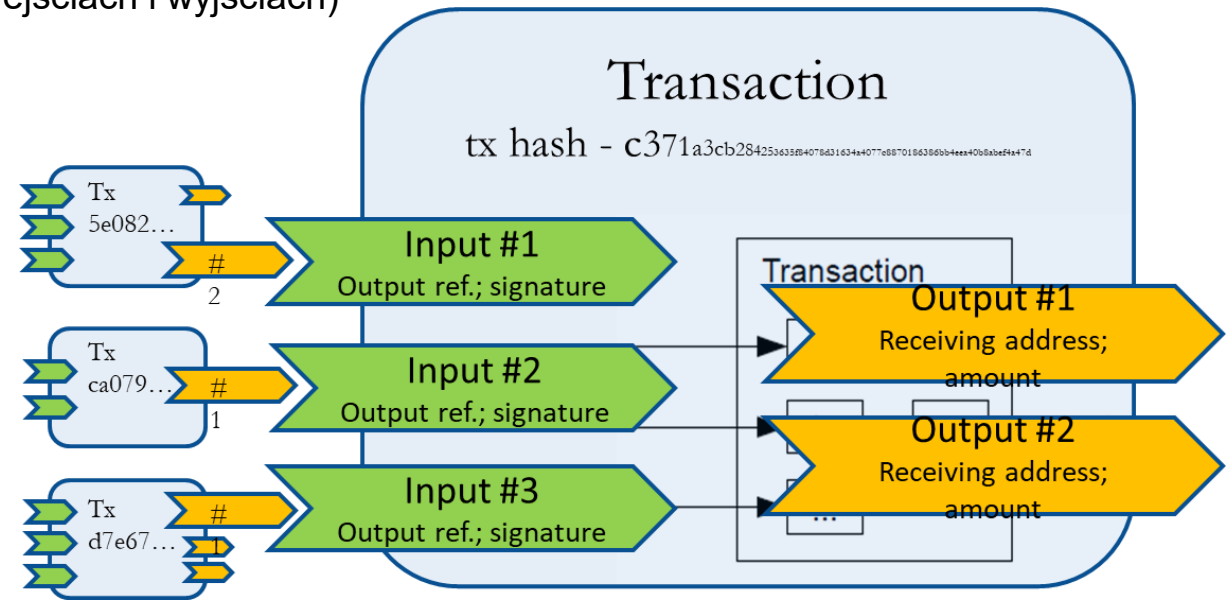
Funkcja skrótu to SHA-256.

Ekran aplikacji klienta Bitcoin.

Źródło: https://bitcoin.org/en/developer-guide

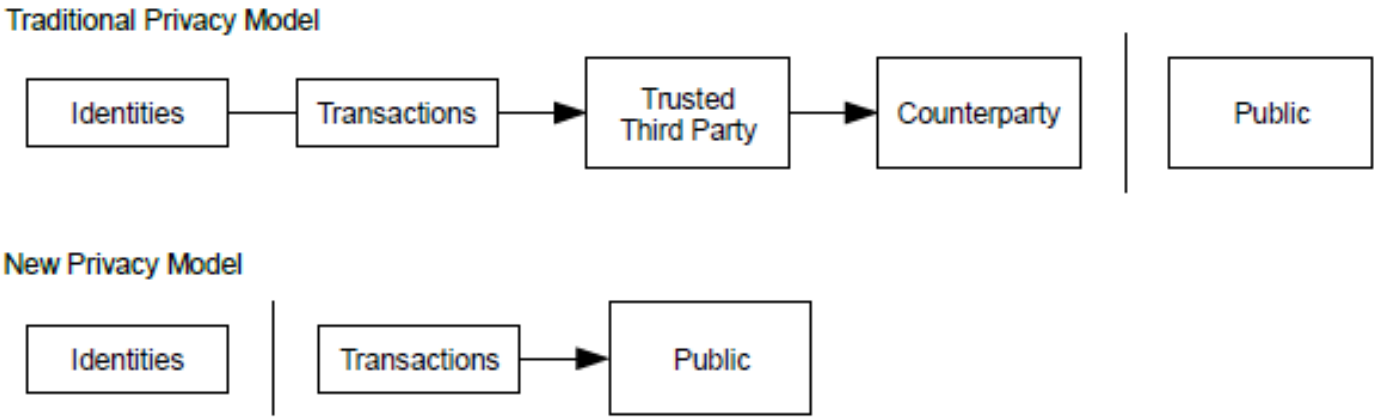
Bitcoin: A Peer-to-Peer Electronic Cash System (cd.)

- **Pierwsza transakcja w bloku to nowe środki (nagroda za wydobycie).**
- **Transakcje mogą zawierać na raz klika wejść i wyjść (aby umożliwić podział środków):**
  - Zazwyczaj będzie to jedno wejście pochodzące z jednej dużej poprzedniej transakcji lub wiele wejść z małymi kwotami z kilku transakcji.
  - Zwykle będą istniały dwa (lub trzy) wyjścia: jedno dla odbiorcy przesyłanej „monety”, drugie z resztą dla płacącego oraz trzecie z prowizją dla wydobywających bloki.
  - Nigdy nie istnieje potrzeba pozyskiwania listy poprzednich transakcji (mogłoby to być trudne przy wielu wejściach i wyjściach)



Bitcoin: A Peer-to-Peer Electronic Cash System (cd.)
Model zaufania

- **W standardowym modelu bankowości prywatność jest osiągana poprzez limitowanie dostępu do danych bankowych.**
- **W Bitcoin klucze publiczne są anonimowe. Wszyscy widzą, że ktoś wysyła pieniądze do kogoś innego, ale bez informacji łączącej transakcji z konkretną osobą (podobnie jak informacje giełdowe).**
- **Dodatkowo zaleca się, aby dla każdej transakcji została użyta nowa para kluczy, tak aby nie można ich było połączyć z jednym właścicielem. W przypadku transakcji wielowejściowych transakcje są grupowane razem i wskazują na jednego właściciela.**

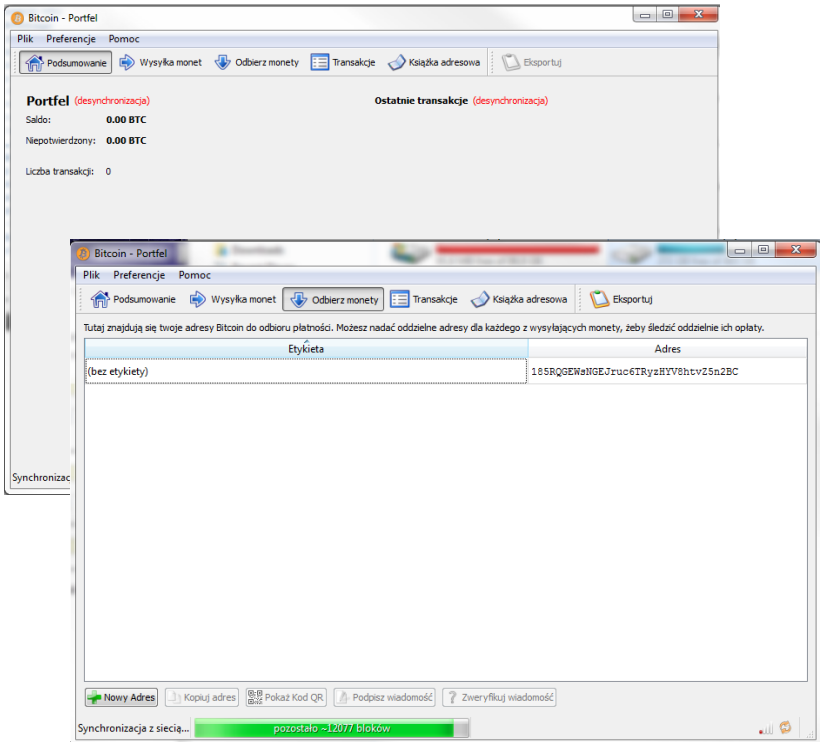


Plan wykładu

1. Wstęp, co to jest Blockchain?
2. Bitcoin
3. **Bitcoin w praktyce**
4. Blockchain a wymagania bezpieczeństwa
5. Podsumowanie

Bitcoin – w praktyce 1/6

- **Aby odbierać i wysyłać Bitcoin potrzebna jest aplikacja portfela.**
- **Istnieje wiele aplikacji portfela, m. in:**

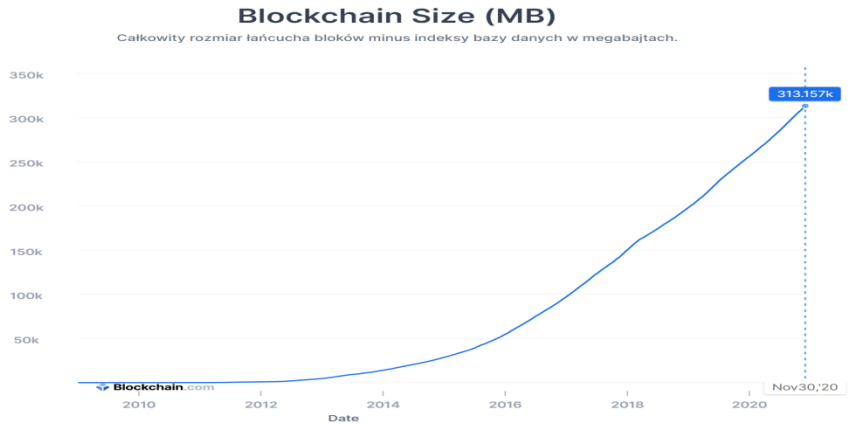


Windows Wallets	Control	Validation	Transparency	Environment	Privacy	Fees
Armory	●	●	◢	▲	●	●
Bitcoin Core	●	●	●	▲	●	●
Bitcoin Knots	●	●	●	▲	●	●
Bither	●	◢	◢	▲	◢	▲
BitPay	●	▲	◢	▲	◢	◢
Electrum	●	◢	◢	◢	◢	●
mSIGNA	●	●	◢	▲	●	▲
Wasabi	●	▲	●	▲	●	◢

● Good ◢ Acceptable ▲ Caution ■ Neutral

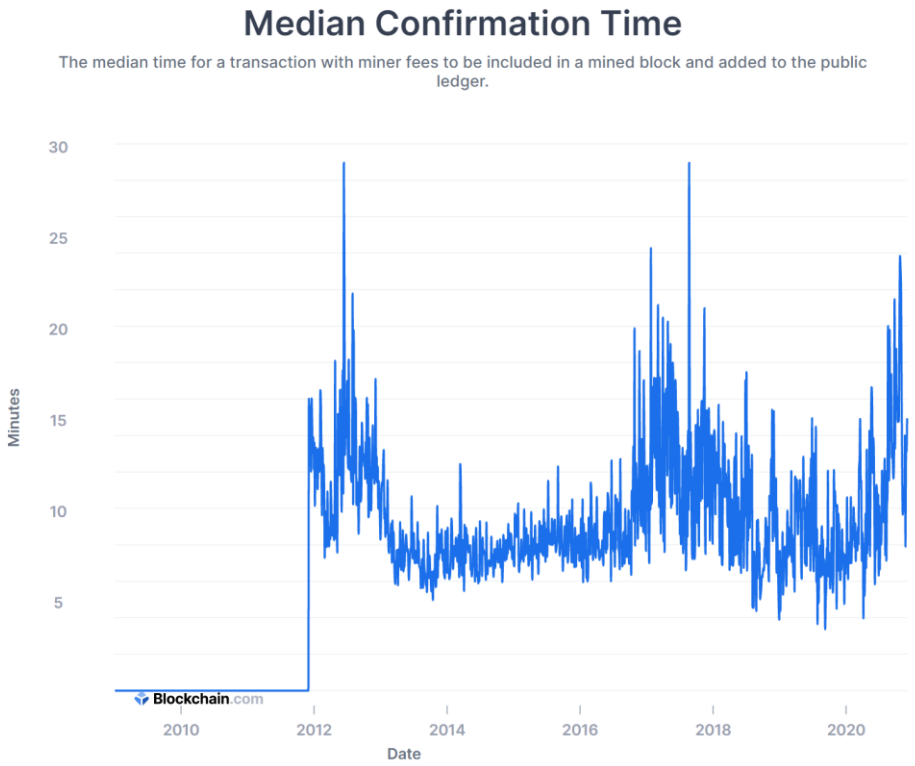
Bitcoin – w praktyce 2/6

- **Portfele offline wymagają ściągnięcia całego łańcucha bloków Bitcoin'a, którego rozmiar to obecnie 377GB.**
- **Niektóre portfele wykorzystują serwisy, takie jak blockchain.com, do weryfikacji blockchain'a (ale wymaga to zaufania do tego serwisu, co powoduje utratę właściwości braku konieczności zaufania)**
- **Portfele online – środki trzymane są na koncie usługodawcy, dostęp do środków zależy tylko od usługodawcy (pod względem modelu zaufania jest to gorszy wariant niż tradycyjna bankowość, gdyż musimy ufać usługodawcy, a nie mamy żadnych gwarancji prawnych odnośnie przechowywyanych środków)**



Bitcoin – w praktyce 3/6

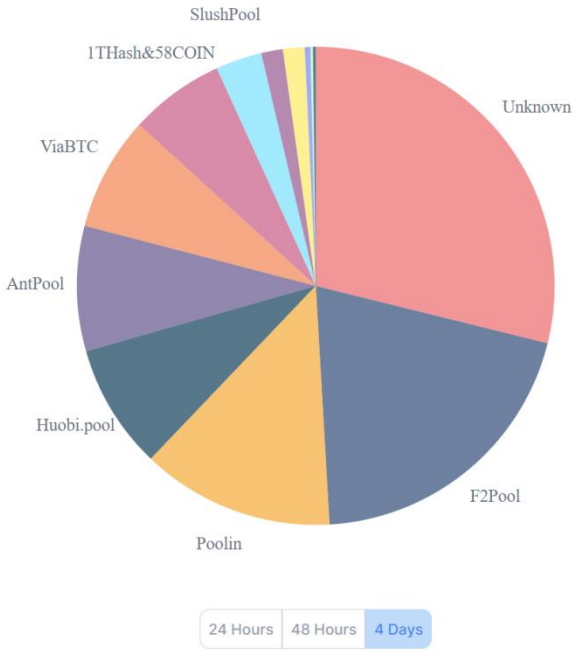
- **Czas zatwierdzenia transakcji to około 10 minut**
- **Powszechnie przyjmuje się, że 6 bloków wystarczy aby uznać transakcje za wbudowaną na stałe do blockchain'a, czyli uznać za zaakceptowaną**



Bitcoin – w praktyce 4/6

- **Obecnie na pojedynczym komputerze nie da się wydobywać nowych bloków (tj. w mechanizmie PoW znaleźć ciąg bitów z odpowiednią liczbą „zer” na początku) ze względu na ogromne wymagania obliczeniowe**
- **Osoby kopiące (kopacze/górnicy) łączą się w zespoły (kopalnie), w których rozdziela się pracę i w przypadku wydobycia bloku dzieli się otrzymane Bitcoiny proporcjonalnie do wniesionego wkładu obliczeniowego**

Miner / Pool	Blocks Mined
Unknown	157
F2Pool	110
Poolin	71
Huobi.pool	46
AntPool	46
ViaBTC	42
1THash&58COIN	35
SlushPool	17



Bitcoin – w praktyce 5/6

Bitcoin – w praktyce 6/6

Bitcoin Block Reward Halving Countdown

Days Hours Minutes Seconds

1251:10:49:26

Reward-Drop ETA date: **08 May 2024 03:45:15 UTC**

Past halving event dates

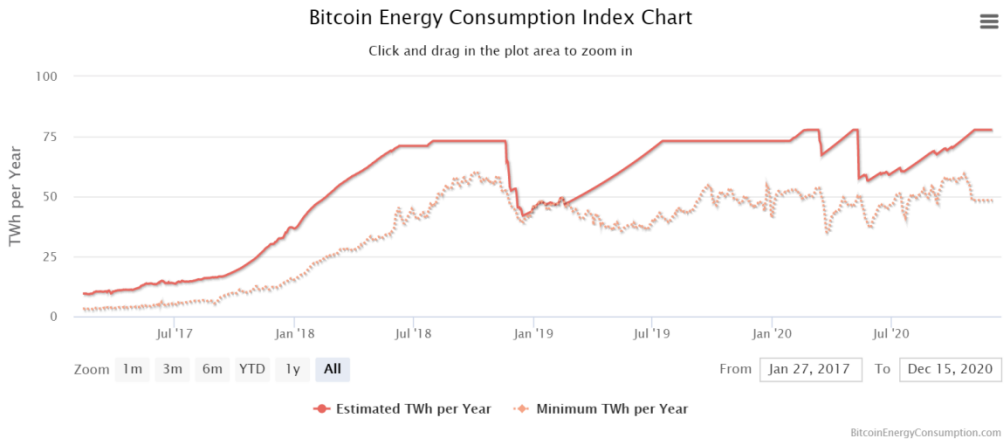
- The first halving event occurred on the 28th of November, 2012 (UTC) at block height 210,000
- The second halving event occurred on the 9th of July, 2016 (UTC) at block height 420,000
- The third halving event occurred on the 11th of May, 2020 (UTC) at block height 630,000

Total Bitcoins in circulation:	18,561,194
Total Bitcoins to ever be produced:	21,000,000
Percentage of total Bitcoins mined:	88.39%
Total Bitcoins left to mine:	2,438,806
Total Bitcoins left to mine until next blockhalf:	1,126,306
Bitcoin price (USD):	$19,410.17
Market capitalization (USD):	$360,276,012,713.12
Bitcoins generated per day:	900

`https://www.bitcoinblockhalf.com/`

Bitcoin – wady 1/5

Zużycie energii więcej niż Polska! , ok 0,5% światowego zużycia!!!



ownload data.

Annualized Total Footprints

Carbon Footprint	Electrical Energy	Electronic Waste
36.95 Mt CO2	77.78 TWh	10.32 kt
Comparable to the carbon footprint of New Zealand.	Comparable to the power consumption of Chile.	Comparable to the e-waste generation of Luxembourg.

https://digiconomist.net/bitcoin-energy-consumption

Bitcoin – wady 2/5

Single Transaction Footprints

Carbon Footprint

321.55 kgCO2

Equivalent to the carbon footprint of **712,663** VISA transactions or **53,591** hours of watching Youtube.

Electrical Energy

676.94 kWh

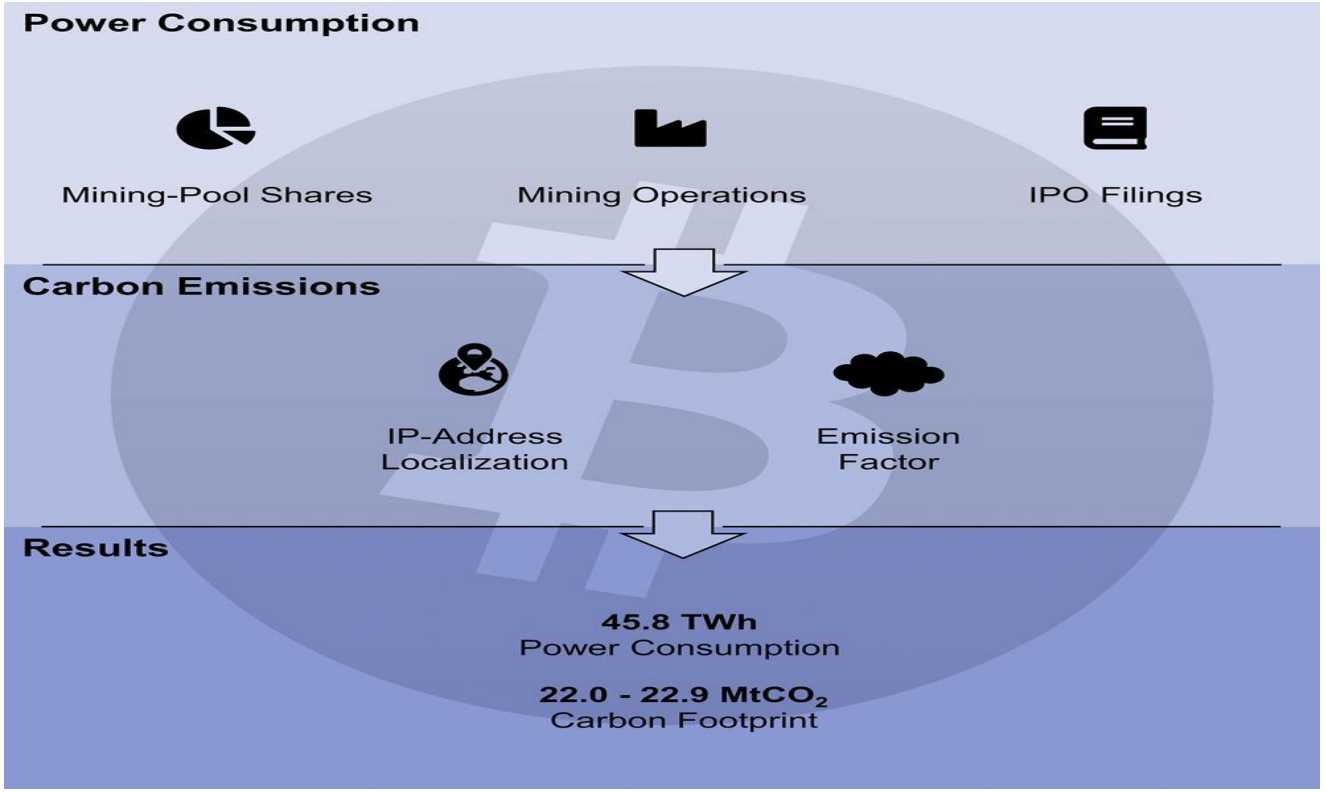
Equivalent to the power consumption of an average U.S. household over **23.20** days.

Electronic Waste

89.90 grams

Equivalent to the weight of **1.38** 'C'-size batteries or **1.96** golf balls. (Find more info on e-waste here.)

Bitcoin – wady 3/5



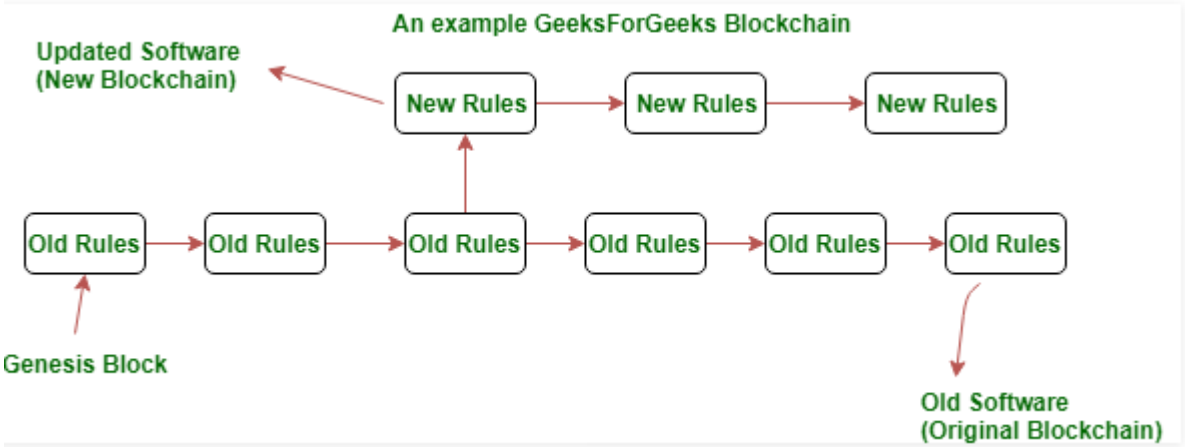
https://www.sciencedirect.com/science/article/abs/pii/S2542435119302557

Bitcoin – wady 4/5

- **Bitcoin powinien być zdecentralizowany. Jednakże kopanie nowych Bitcoinów jest coraz bardziej scentralizowane, co zwiększa szanse na pozyskanie większości mocy obliczeniowej (*51% attack*) oraz *selfish mining attack***
  - ***selfish mining attack* – zamiast publikować wydobyty blok, kopacz zatrzymuje go dla siebie i liczy następny, podczas gdy konkurenci tracą moc obliczeniową na obliczanie starego bloku; po pewnym czasie publikuje on dłuższy łańcuch, który staje się obowiązujący, atak działa wtedy, gdy kontroluje się co najmniej około 1/3 mocy obliczeniowej sieci**
  - **W lipcu 2014 GHash.IO posiadał więcej niż 50% mocy wydobywczej**
- **Kryptowaluty nie są koordynowane, trudno dokonać zmiany w protokole, np. by zwiększyć liczbę transakcji, konieczna jest zgoda prawie wszystkich węzłów (poza tym np. Bitcoin nie ma spisanej specyfikacji – działająca wersja jest uznana za obowiązującą…)**

Bitcoin – wady 5/5

- **Błędy w oprogramowaniu Bitcoin'a mogą spowodować, że łańcuch zostanie odrzucony - nawet 6 zaakceptowanych bloków nie gwarantuje, że transakcja pozostanie w łańcuchu bloków**
  - **Błędy historyczne: CVE-2010-5139, „bug" podczas zmiany wersji z 0.7 na 0.8**
- **Domyślne założenie, że Bitcoin nie wymaga zaufania, jest nie do końca oczywiste, m.in. wymagane jest pewne zaufanie do dostawców oprogramowania.**
- **Powstawanie „rozwidleń" (forks) łańcucha bloków:**



Soft Fork: gdy protokół blockchain jest zmieniany w sposób zgodny z poprzednimi wersjami;
Hard Fork: gdy protokół blockchain jest zmieniany w sposób niezgodny z poprzednimi wersjami;
Temporary Fork: gdy dwóch górników wydobywa jednocześnie nowy blok.

Źródło: https:// www.geeksforgeeks.org/blockchain-forks/

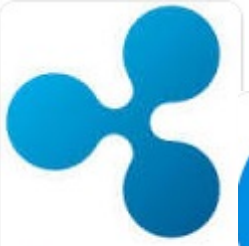
Kryptowaluty „na start”

Bitcoin

Ethereum

Bitcoin Cash

Dogecoin



Ripple

Dash

Monero

NEM

PotCoin

Primecoin

Peercoin

Cardano

Plan wykładu

1. Wstęp, co to jest Blockchain?
2. Bitcoin
3. Bitcoin w praktyce
4. **Blockchain a wymagania bezpieczeństwa**
5. Podsumowanie

Blockchain – wymagania bezpieczeństwa

Wymagania dotyczące integralności

- **Agreement on Transaction Validity – tylko prawidłowa transakcja może być zapisana w rejestrze, w zależności od semantyki transakcji.**

- **Tamper Evidence - rejestr powinien być odporny na naruszenia oraz musi być spójny wśród uczestników (cecha DLT – Distributed Ledger Technology – wykrywanie naruszeń wtedy, gdy węzeł może porównać wartość skrótu transakcji z innymi węzłami w celu wykrycia takich naruszeń).**

- **Finality - żadna transakcja nie może zostać odrzucona po jej zatwierdzeniu i zarejestrowaniu w rejestrze.**

Blockchain – wymagania bezpieczeństwa

Wymagania dotyczące prywatności

- **C1: Anonymity to Third Parties – Tożsamość podmiotów obrotu nie jest widoczna dla stron innych niż kontrahenci transakcji.**
- **C2: Anonymity between Counterparties: Dodatkowo w stosunku do C1, tożsamości podmiotów uczestniczących w transakcji nie są widoczne nawet pomiędzy kontrahentami.**
- **C3: Confidentiality of Transaction Content: Poufność informacji o treści transakcji.**
- **C4: Confidentiality about Existence of Transaction: Poufność informacji o zaistnieniu transakcji.**
- **C5: Confidentiality of State: Poufność informacji o stanie łańcucha bloków (znane są tylko wartości odpowiednich skrótów).**

Blockchain – wymagania bezpieczeństwa

- **Bitcoin i inne kryptowaluty spełniają tylko probabilistycznie właściwości *Finality***
  - **Innymi słowy transakcje nie są niezaprzeczalne**

Unspent Transaction Output

	Bitcoin	Ethereum	Quorum	Corda	Fabric V0.6	Fabric V1.0	
Data Structure	Block	Block + State	Block + State	State	Block + State	Block + State	
Transaction Process	UTXO	Smart Contract (Solidity/EVM)	Smart Contract (Solidity/EVM)	UTXO (+Java flow)	Smart Contract (Go, Java)	Smart Contract (Go)	
Consensus	PoW	PoW	QuorumChain, Raft	Notary (Raft, BFT-SMaRt)	PBFT	Fabric Consensus	
Integrity Requirements							
I1:Transaction Validity	Yes when $f<N/2$	Yes when $f<N/2$	*(based on vote threshold)*	Agreement bet. counterparties	Yes when $f \leqq (N-1)/3$	Yes when $f<N/2$	
I2: Tamper Resistance	Yes when $f<N/2$	Yes when $f<N/2$	Yes when $f<N/2$	No	Yes when $f \leqq (N-1)/3$	Yes when $f<N/2$	
I3: Finality	No (probabilistic)	No (probabilistic)	Yes (*1)	Yes (*1)	Yes	Yes (*1)	
Privacy Requirements						Single Ch.	Multi Ch.
C1: Anonymity to third party	Yes	Yes	Yes	Yes	Yes (*2)	No	Yes
C2: Anonymity between counterparties	Yes	Yes	No	Yes	Yes (*2)	No	Yes
C3:Tx content confidentiality	No	No	Yes	Yes	Yes (*3)	Yes(*3)	Yes
C4:Tx existence confidentiality	No	No	No	Yes	No	No	Yes
C5: State confidentiality	N/A	No	Yes	Yes	Yes (*3)	Yes(*3)	Yes

Blockchain – zastosowania poza kryptowalutami

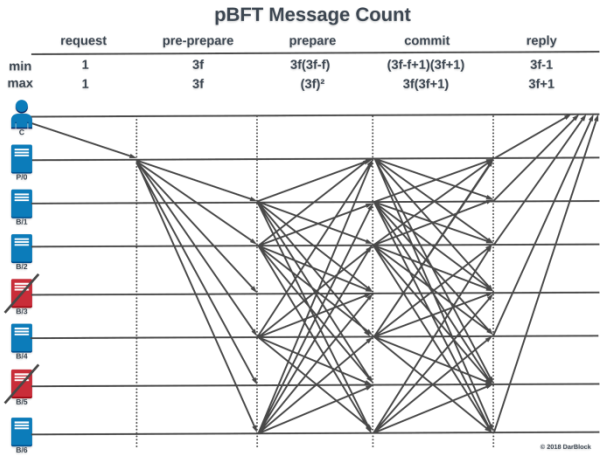
- **Mechanizm Proof-of-Work sprawdza się w zasadzie tylko w przypadku kryptowalut.**
- **W innych zastosowaniach technologii blockchain (zapewnienie integralności dokumentów, transakcji/kontraktów, czy np. zbiorów danych cyfrowych takich jak dane medyczne) stosuje się inne mechanizmy konsensusu, np.:**
  - **PBFT – Practical Byzantine Fault Tolerant**
  - **PoA – Proof-of-Authority**
  - **PoS – Proof-of-Stake**
  - **PoB – Proof-of-Burn**
  - **Itd., itp**

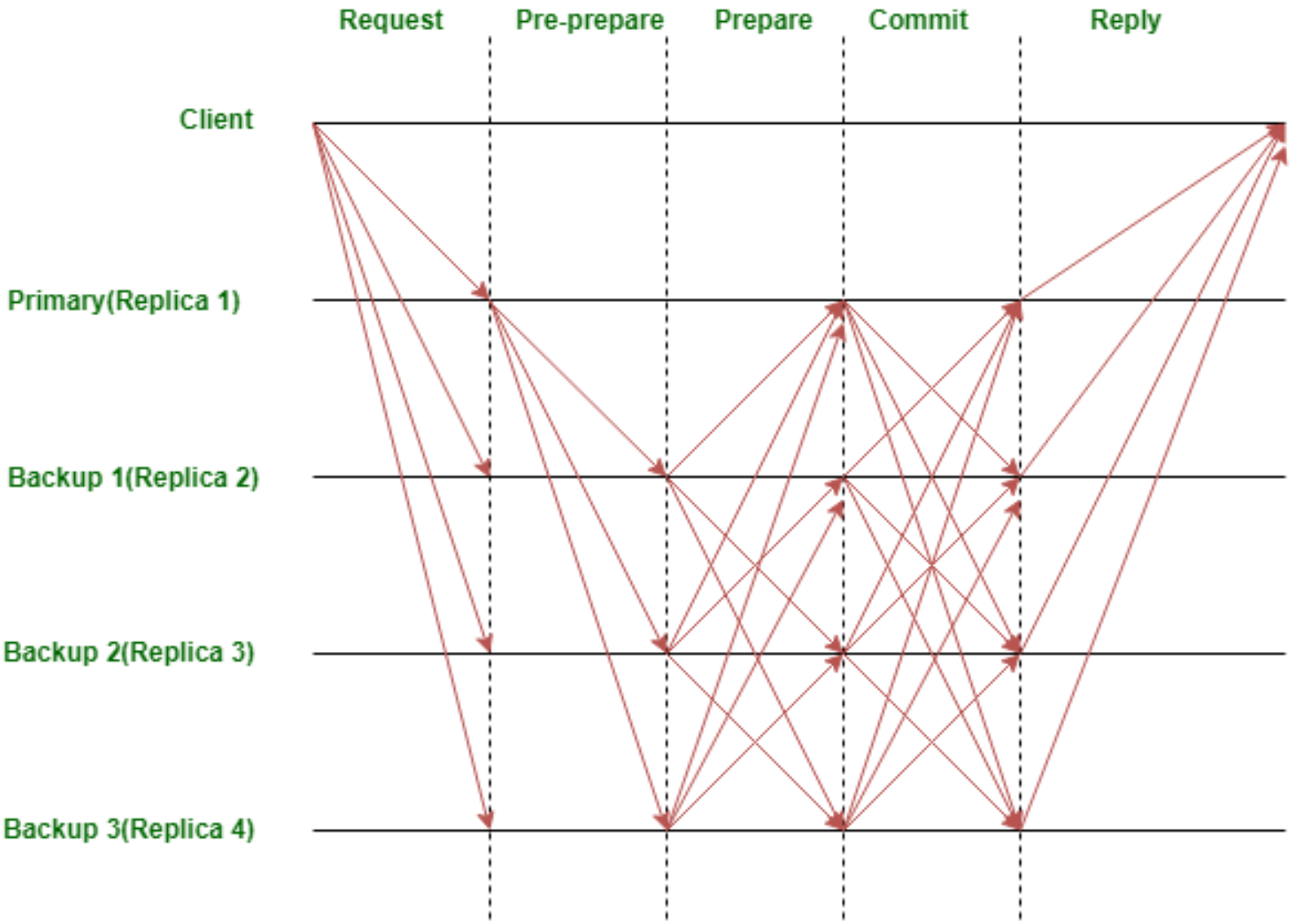
Blockchain – PBFT

- **BFT (Byzantine Fault Tolerance) to mechanizm konsensusu nawiązujący do Problemu Bizantyjskich Generałów (jak uzgodnić wspólną decyzję w sytuacji, gdy część „węzłów/generałów” rozsyła sprzeczne komunikaty z oryginalnym komunikatem, bądź wcale nie przekazuje oryginalnego komunikatu, a decyzję podjąć trzeba; tą decyzją jest dołączenie lub nie kolejnego bloku do łańcucha).**
- **BFT może zapewnić odporność sieci na błędy, pozwalając jednocześnie na przetwarzanie tysięcy operacji na sekundę z niemal znikomym wydłużeniem czasu oczekiwania.**
- **Praktyczna Bizantyjska Tolerancja Błędów (PBFT) jest przypadkiem szczególnym i optymalnym rozwiązania tego problemu.**
- **Protokół został zaproponowany w 1999 roku przez Miguela Castro i Barbarę Lisk.**
- **PBFT posiada zdolność do jednoznacznego osiągnięcia konsensusu, pomimo prób rozsyłania fałszywych danych do innych użytkowników przez złośliwe węzły.**

Blockchain – PBFT

- **Wszystkie węzły w PBFT są ustawione w sekwencje, w których jeden węzeł jest liderem (leader) a pozostałe są węzłami zapasowym (backup nodes)**
- **Uczciwe węzły komunikują się ze sobą wzajemnie i muszą ustalić wspólny stan – liczba wiadomości zwiększa się wykładniczo ze wzrostem liczby węzłów**
- **Wymagane jest sprawdzenie, czy wiadomość pochodzi od konkretnego węzła i czy nie została zmodyfikowana podczas transmisji**
- **PBFT wymaga minimum *3f + 1* węzłów, gdzie *f* to maksymalna liczba węzłów złośliwych**
- **Protokół nie skaluje się dobrze przy dużej liczbie węzłów**




Request
Pre-prepare
Prepare
Commit
Reply
Client
Primary(Replica 1)
Backup 1(Replica 2)
Backup 2(Replica 3)
Backup 3(Replica 4)

Każda runda mechanizmu konsensusu PBFT sprowadza się do 4 faz:

1. **Klient wysyła żądanie do węzła wiodącego (Primary).**
2. **Węzeł wiodący przekazuje żądanie do węzłów drugorzędnych (Secondary/Backup).**
3. **Węzły obsługują żądanie (np. sprawdzają poprawność semantyki i integralność żądania, a następnie wysyłają odpowiedź do klienta).**
4. **Klient oczekuje na f + 1 (f oznacza maksymalną liczbę węzłów, która może być wadliwa), odpowiedzi z różnych węzłów z tym samym wynikiem.**

Węzeł wiodący (leader) zmienia się po każdej rundzie zgodnie z zasadą „Round Robin”. Może zostać także zastąpiony przez węzeł zapasowy (backup node) wtedy, gdy „zwleka” z przekazaniem żądania do węzłów zapasowych.

Blockchain – Proof-of-Authority

- **Transakcje i bloki są zatwierdzane przez autoryzowane węzły.**
- **Zaufane węzły uruchamiają oprogramowanie umożliwiające im umieszczanie transakcji w blokach; proces jest zautomatyzowany.**
- **PoA nadaje się zarówno do sieci prywatnych, jak i publicznych, gdzie zaufanie jest rozproszone.**
- **Istnieje lista autoryzowanych węzłów oraz protokół umożliwiający aktualizację tej listy, tj. dodawanie nowych węzłów oraz usuwanie węzłów nieuczciwych**
- **Wymienianych jest mniej wiadomości niż w PBFT.**
- **Osiągnięcie spójności w PoA może być problematyczne, w przeciwieństwie do PBFT, gdzie dostępność nie jest gwarantowana, a spójność jest osiągana zawsze.**

Plan wykładu

1. Wstęp, co to jest Blockchain?
2. Bitcoin
3. Bitcoin w praktyce
4. Blockchain a wymagania bezpieczeństwa
5. **Podsumowanie**

Blockchain – Podsumowanie

- **Blockchain nie jest magicznym narzędziem leczącym wszystkie problemy informatyki…**
- **Kryptowaluty w praktyce nie posiadają cech zdecentralizowania i braku zaufania do zaufanego podmiotu trzeciego…**
- **Mechanizmu PoW nie da się zastosować w prywatnych blockchain'ach**
- **W prywatnych blockchain'ach stosuje się PBFT lub PoA lub ich odmiany**
- **Najpopularniejsze oprogramowanie open-source implementujące prywatny blockchain to HyperLedger Fabric**
- **Istnieją sposoby wykorzystania Bitcoin'a do tworzenia znaczników czasu (np. OpenTimeStamps), ale czy znaczniki te będą niezaprzeczalne?**
  - **skrót z dokumentu wstawia się jako publiczny adres odbiorcy pieniędzy w transakcji, kwota transakcji jest przepalana (tracona), a czas to moment wydobycia bloku (można to sprawdzić np. na blockchain.info)**
- **Nadchodzi komputer kwantowy…**

Koniec części 9