

“
ANY SUFFICIENTLY ADVANCED
TECHNOLOGY IS
INDISTINGUISHABLE FROM MAGIC”

Arthur C. Clarke

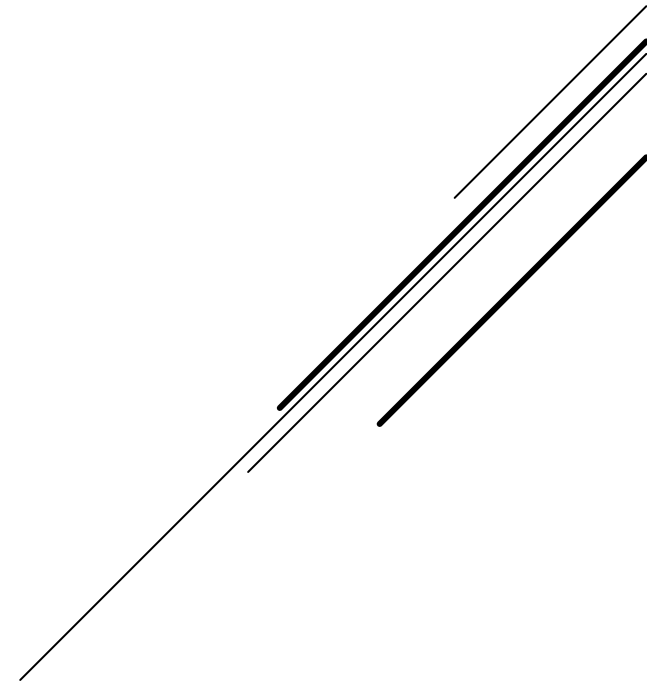
TEORIA

dr inż. Przemysław RODWALD

tłum.: „Każda wystarczająco zaawansowana technologia jest nierozróżnialna od magii.”

- A. Zasada działania kryptowalut, łańcuch bloków
- B. Klucze, adresy, transakcje
- C. Pseudoanonimowość

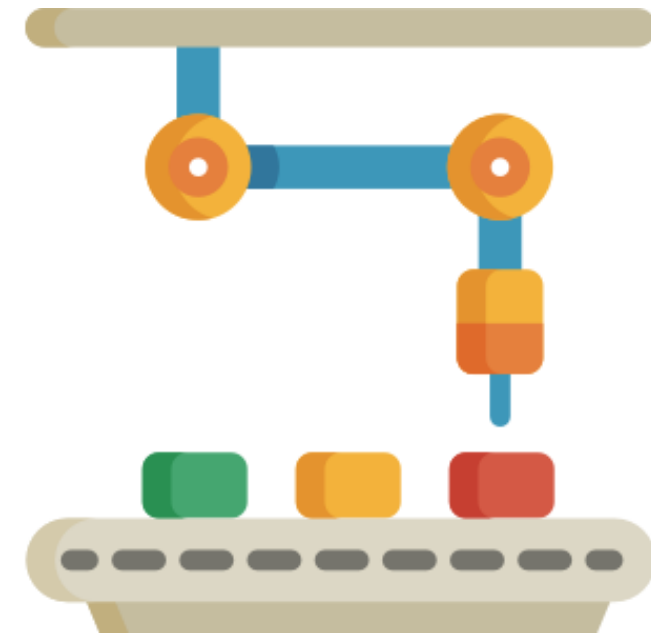
PLAN PREZENTACJI



Na podstawie:

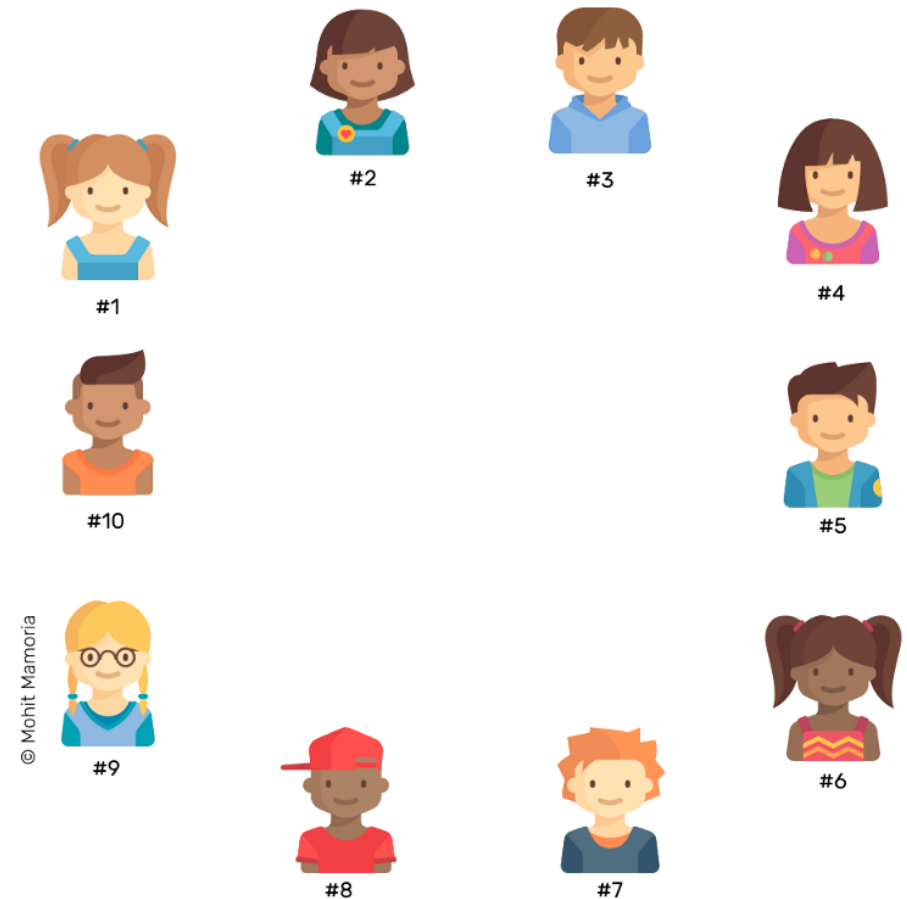
- ▶ <https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348>

A. „BLOCKCHAIN” NAJPROŚCIEJ



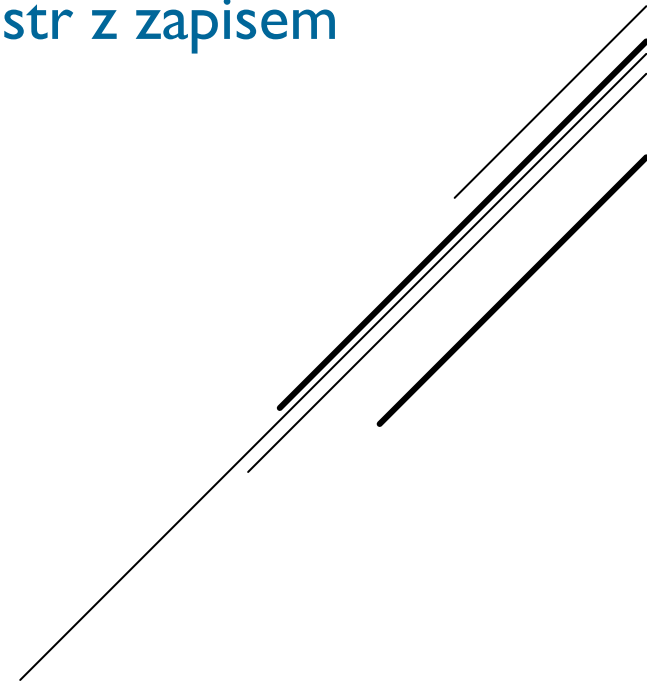
- ▶ założmy, że 10 osób chce przestać korzystać z usług banków ale móc wymieniać między sobą pieniądze
- ▶ wszyscy zgadzają się, że będą nieustannie gromadzić i przechowywać szczegóły wszystkich transakcji w sieci
 - ▶ bez potrzeby przechowywania danych dotyczących swojej tożsamości (stąd numeracja)

SCENARIUSZ



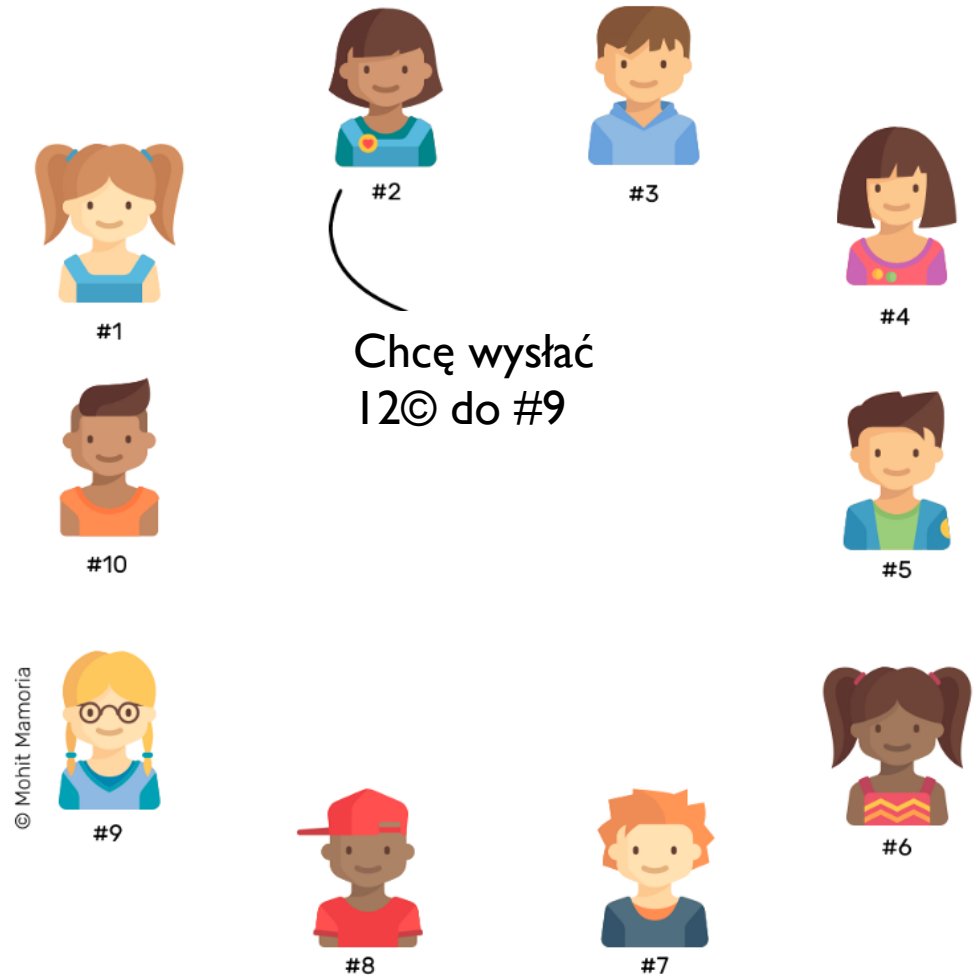
- ▶ każdy na początek ma pusty segregator
- ▶ w miarę jak będą dokonywane transakcje każda z osób będzie do swojego segregatora dodawać kolejne numerowane kartki
- ▶ ten segregator (uporządkowany zbiór kartek) będzie tworzył rejestr z zapisem wszystkich transakcji

I. PUSTY SEGREGATOR



- ▶ Każdy weźmie czystą kartę i długopis i przygotowuje się do zapisania każdej transakcji jakie będą miały miejsce w ramach całego systemu.
- ▶ #2 chce przesłać 12© do #9:
 - ▶ aby doszło do transakcji #2 rozgłasza wszystkim:
 - ▶ „Chcę wysłać 12 © do #9. Zapiszcie wszyscy na swoich kartach.”
 - ▶ każdy sprawdza, czy #2 ma wystarczająco środków, żeby przesłać 12 © do #9
 - ▶ jeśli tak, każdy zapisuje, że doszło do takiej transakcji
 - ▶ jeśli nie odrzuca transakcję

© - „nasz_coin” – waluta obowiązująca w tym systemie

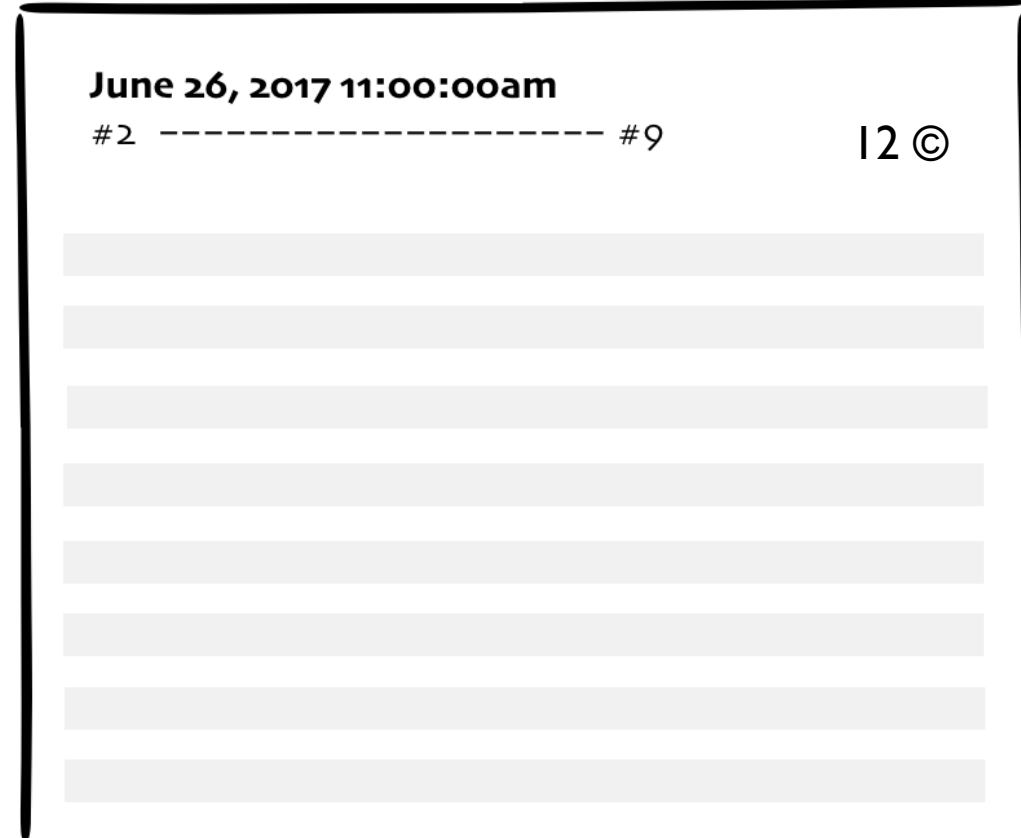


2. TRANSAKCJA

Pytanie: Czy wszyscy widzą transakcje innych użytkowników?

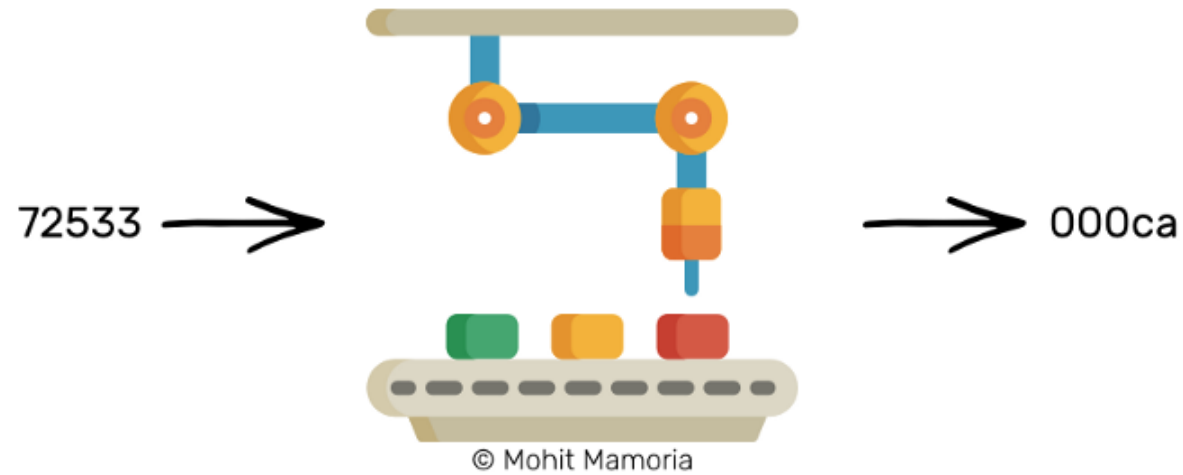
- ▶ W sieci mają miejsce kolejne transakcje.
- ▶ Każda jest zapisywana przez wszystkich na swojej kartce.
- ▶ Gdy skończy się miejsce na kartce każdy odkłada ją do segregatora i bierze nową kartkę.
- ▶ Przed odłożeniem kartki do segregatora należy ją zapieczętować unikalnym kluczem, który wszyscy użytkownicy sieci wspólnie ustalą
 - ▶ Ale jak to zrobić?
 - ▶ Użyjemy „magicznej maszyny”

3. ZAPEŁNIENIE KARTKI

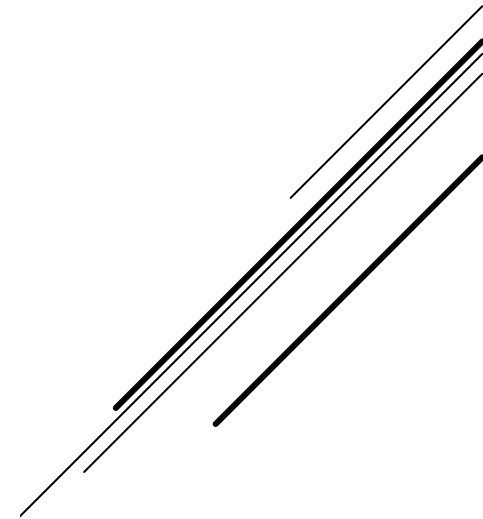


BRAK MIEJSCA NA KARCIE

„MAGICZNA MASZYNA” CZYLI KRYPTOGRAFICZNA FUNKCJA SKRÓTU



.....

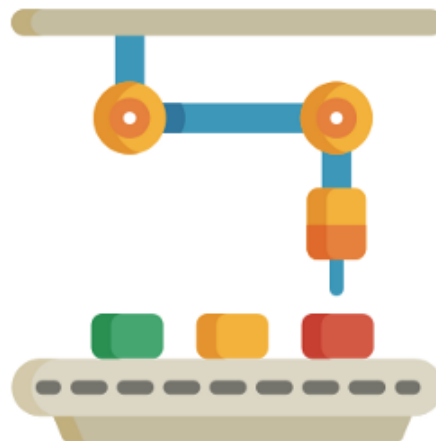
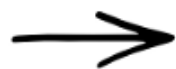


4. ZAPIECZĘTOWANIE KARTKI

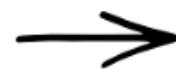
20893

+

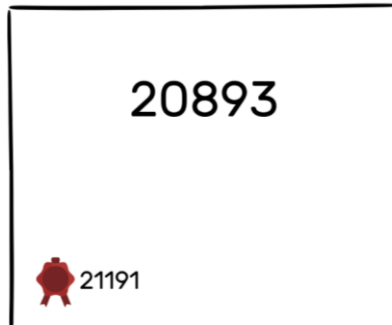
21191



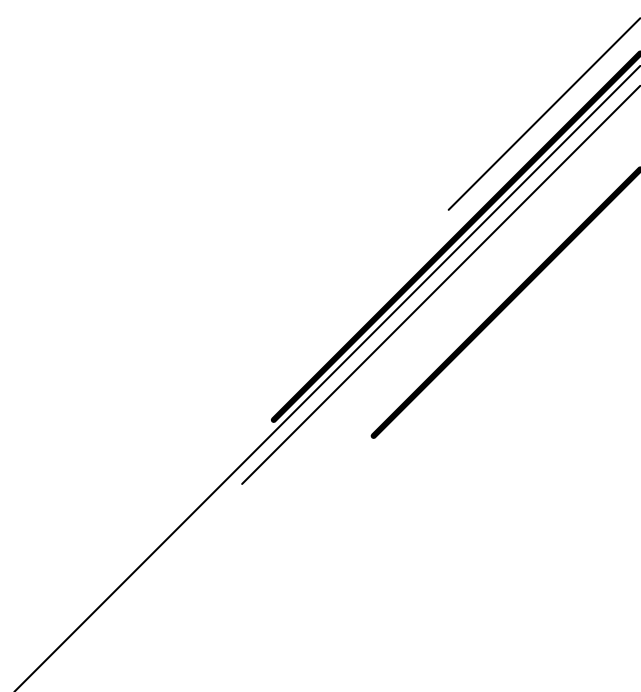
© Mohit Mamoria



00078



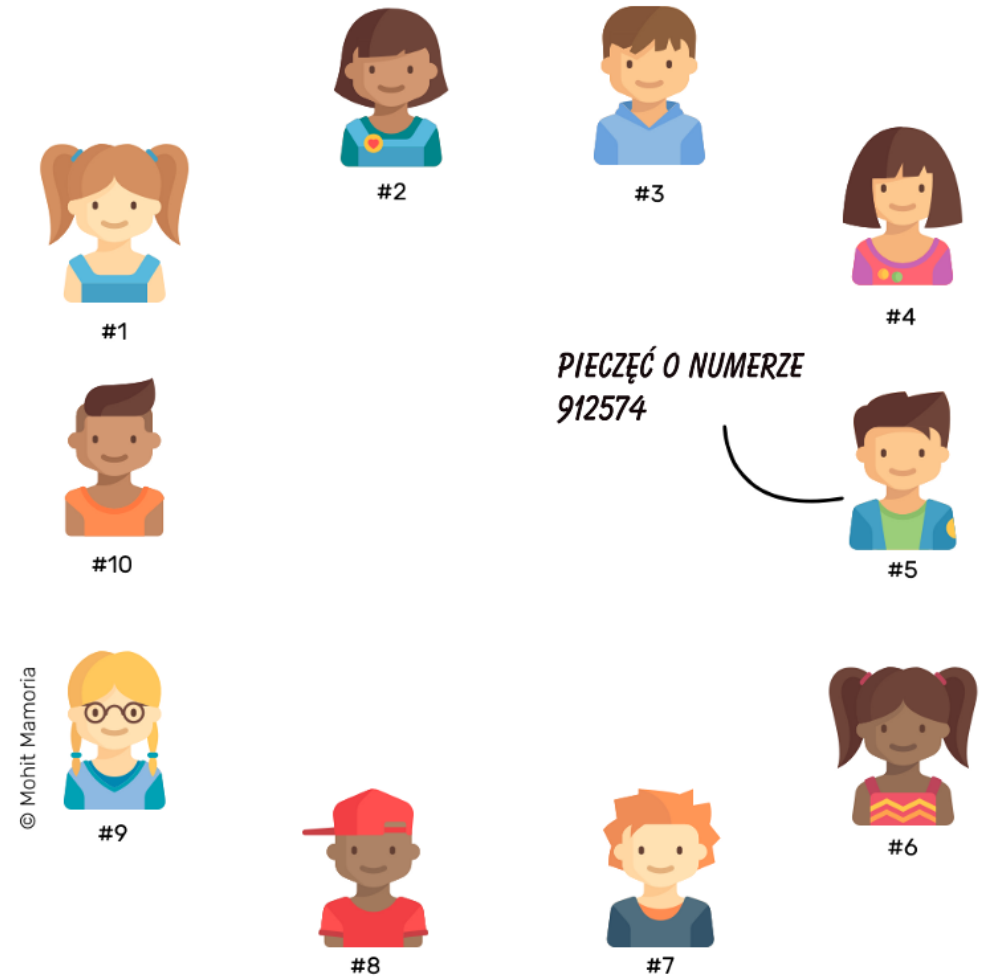
**pieczęć to tzw. „proof of work”
- dowód na to, że podjęto trud
związany z jej wyliczeniem**



- ▶ Gdy skończy się miejsce na kartce wszyscy zaczynają szukać pieczęci.
- ▶ Pierwsza osoba która ją znajdzie informuje o tym inne osoby.
- ▶ Wszystkie osoby sprawdzają czy pieczęć jest prawidłowa.
 - ▶ Jeśli tak, wszyscy pieczętują swoje karty uzyskaną liczbą (pieczęcią) i odkładają je do folderów.
 - ▶ Jeśli jednak u kogoś pieczęć się nie zgadza (na przykład: źle usłyszana transakcja, próba oszustwa) musi on wówczas odrzucić swoją kartkę i pobrać ją od innego użytkownika sieci.

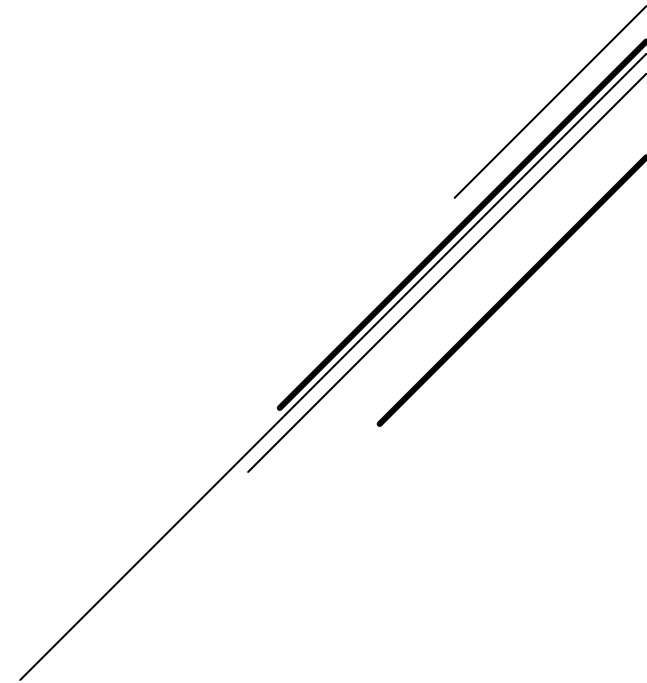
Pieczęć którą wybierze większość uczestników sieci, będzie obowiązująca.

5. PIECZĘTOWANIE

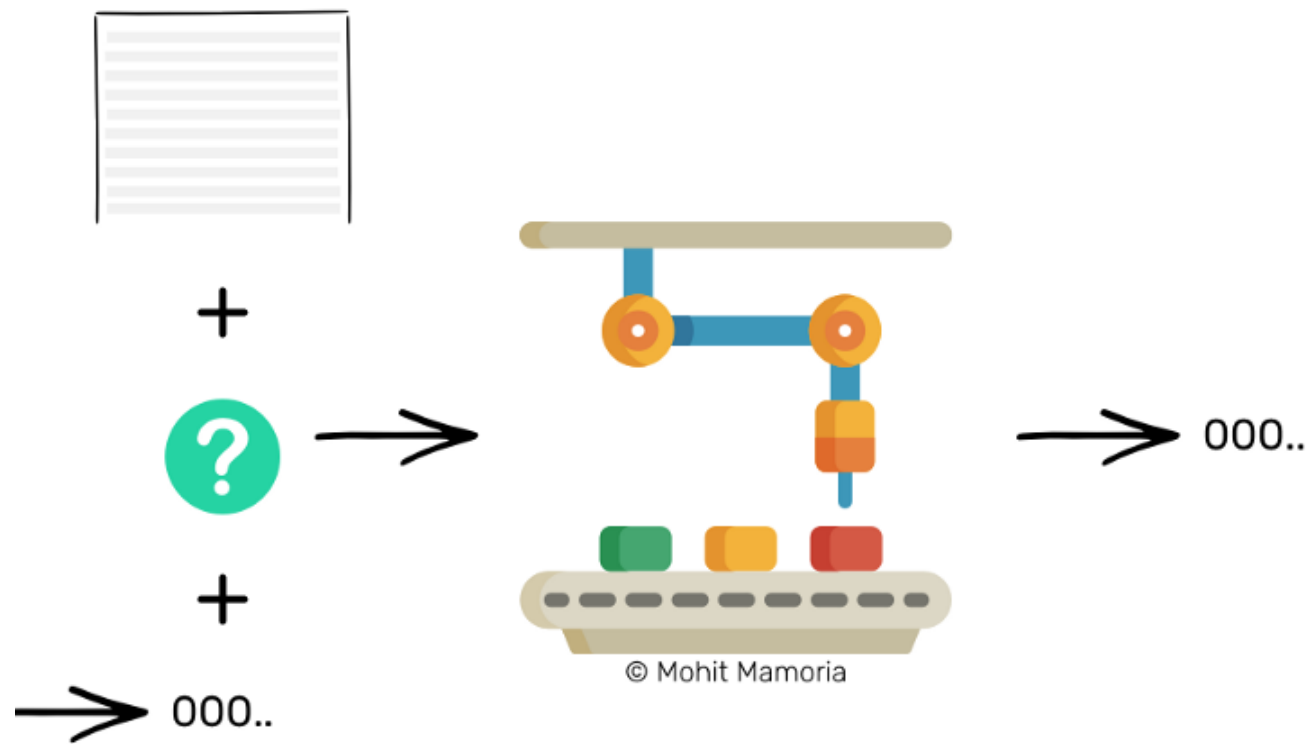


- ▶ Dlaczego każdy uczestnik sieci zużywa zasoby na poszukiwanie pieczęci?
 - ▶ Przecież wiadomo, że ktoś inny wykona te same obliczenia i ogłosi wynik
 - ▶ Może lepiej po prostu poczekać bezczynnie
- ▶ Nagroda
 - ▶ pierwszy który znajdzie pieczęć otrzymuje zapłatę
 - ▶ na przykład 2 © w naszym scenariuszu
 - ▶ jest ona „wytworzona z powietrza”, powiększa liczbę monet w systemie

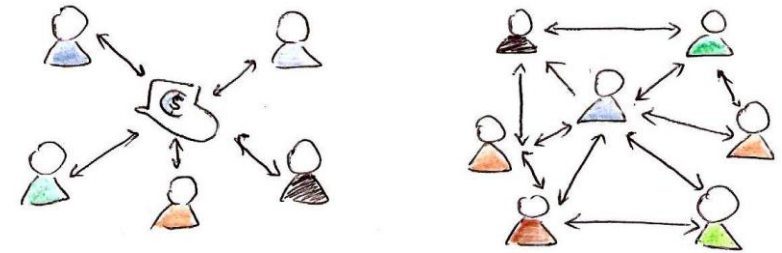
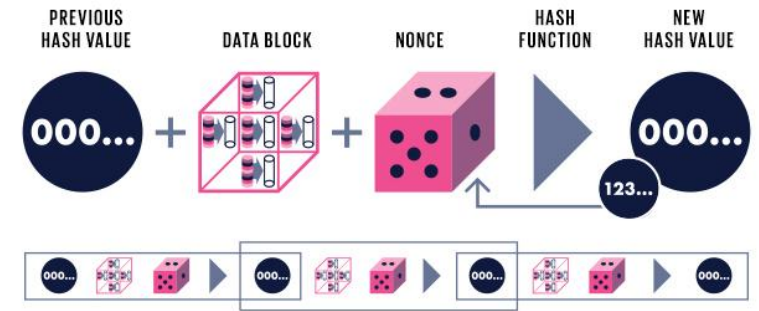
PIECZĘTOWANIE - NAGRODA



OCHRONA PRZED PODMIANĄ KART



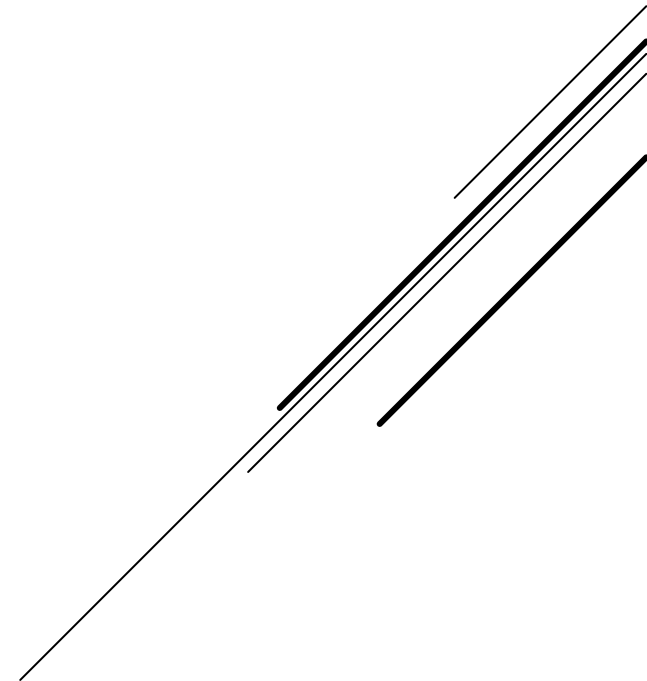
- ▶ Rozproszona baza danych
 - ▶ każdy może posiadać własną bazę (węzeł)
- ▶ Komunikacja P2P
 - ▶ komunikacja odbywa się bezpośrednio między węzłami
- ▶ Pseudoanonimowość
 - ▶ każda transakcja (adresy i kwoty) jest widoczna dla każdego
 - ▶ adresy nie zawierają informacji o ich właścicielach
- ▶ Nieodwracalność zapisów
 - ▶ wprowadzenie zapisów do bazy jest nieodwracalne



MECHANIZM DZIAŁANIA BLOCKCHAIN-A

B. KLUCZE, ADRESY, TRANSAKCJE

NA PRZYKŁADZIE BTC



- ▶ data powstania: 2009
 - ▶ 05.09.2008 upadek Lehman Brothers
 - ▶ 03.01.2009 pierwszy blok
- ▶ autor: Satoshi Nakamoto (?)
 - ▶ 1 BTC = 100 000 000 satoshi
- ▶ model: proof-of-work
- ▶ schemat: wykorzystującego niewydane wyjścia transakcji (ang. Unspent Transaction Output, UTXO)
- ▶ max liczba jednostek waluty: 21.000.000
 - ▶ wszystkie BTC zostaną wydobyte dopiero około roku 2140

BITCOIN [BTC]



- ▶ skrywający się pod pseudonimem Satoshi Nakamoto członek listy mailingowej metzdowd.com 31.10.2008 publikuje swój Manifest
 - ▶ bitcoin.org/bitcoin.pdf

SATOSHI NAKAMOTO ?

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.



- ▶ wiele teorii spiskowych odnośnie autora
- ▶ kilkunastu kandydatów, (niemal) żaden się nie przyznał
- ▶ wiele prób analiz:
 - ▶ lingwistycznej, stylometrycznej, semantycznej, czasu postów
- ▶ 23 kwietnia 2011 SN znika z sieci publikując pożegnanie
 - ▶ „I've moved on to other things. It's in good hands with Gavin [Andresen] and everyone.”
- ▶ Satoshi wykopał przynajmniej 1 mln BTC, które nigdy nie zostały wydane

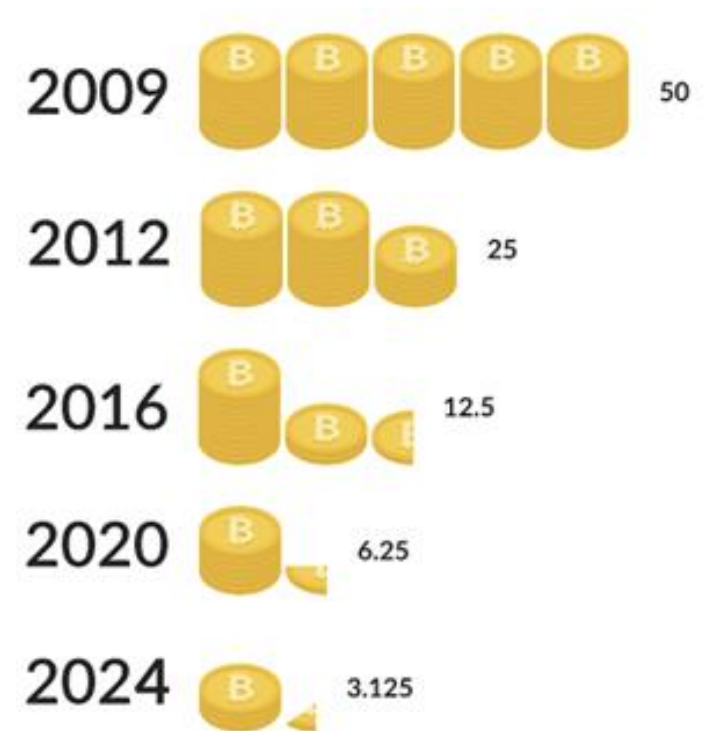
SATOSHI NAKAMOTO ?

1. Jeff Bezos, 177 mld \$
2. Elon Musk, 151 mld \$
4. Bill Gates, 124 mld \$
5. Mark Zuckerberg, 97 mld \$
6. Warren Buffett, 96 mld \$
-
- y. Changpeng Zhao (CEO Binance) 90? mld \$
- ...
- x Satoshi Nakamoto, 40 mld \$

▶ Ile jest wydobywanych BTC?

- ▶ dla pierwszych 210000 bloków nagroda 50 BTC (od 03.01.2009)
 - ▶ dla kolejnych 210000 bloków nagroda 25 BTC (od 28.11.2012)
 - ▶ dla kolejnych 210000 bloków nagroda 12.5 BTC (od 09.07.2016)
 - ▶ dla kolejnych 210000 bloków nagroda 6.25 BTC (od 10.05.2020)
 - ▶ dla kolejnych 210000 bloków nagroda 3.125 BTC (od 20.04.2024)
 - ▶ ...
- ▶ $210000 \cdot (50 + 25 + 12.5 + \dots) \rightarrow 210000000$
- ▶ blok jest wydobywany średnio co 10 minut
- ▶ nowe BTC generowane są *ex nihilo* (z niczego)

SKĄD LICZBA 21 000 000 BTC?



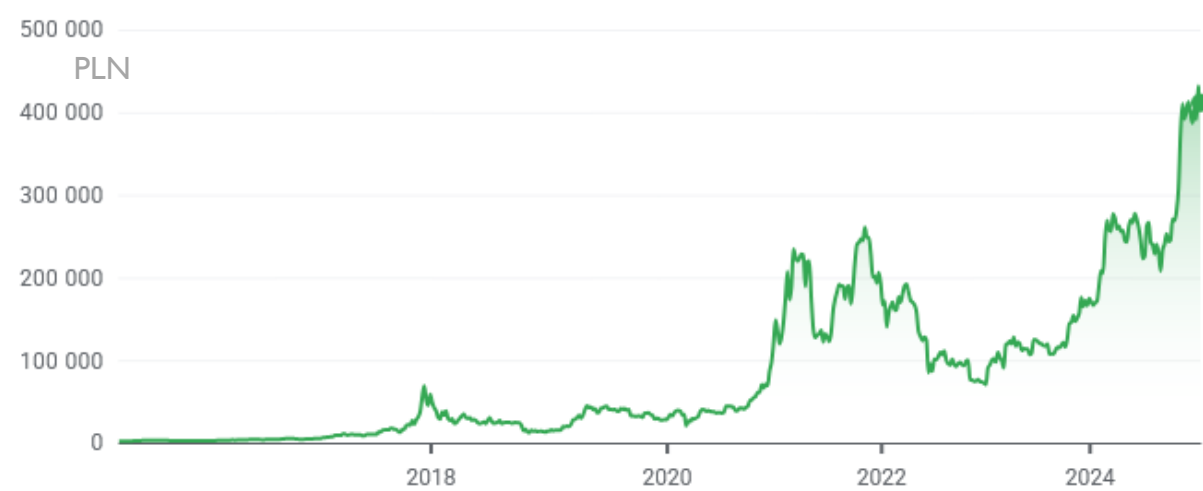
- ▶ Pierwsza transakcja
 - ▶ 3 stycznia 2009 roku o 20:15:05 UTC Satoshi Nakamoto wygenerował pierwszy blok
- ▶ Pierwszy transfer
 - ▶ 12 stycznia 2009 roku Satoshi Nakamoto przesyła 100BTC do Hala Finnera z PGP Corporation
- ▶ Najdroższa pizza (pierwsza? płatność)
 - ▶ 22 maja 2010 roku Laszlo Hanyecz, informatyk z Florydy dał ogłoszenie że zakupi dwie pizze za 10000 BTC (wówczas równowartość około 30\$)
 - ▶ https://en.bitcoin.it/wiki/Laszlo_Hanyecz, Bitcoin Pizza Day
 - ▶ 22 lutego 2010 roku zakup obrazu za 500 BTC (1\$)
 - ▶ <https://pl.beincrypto.com/pierwsze-transakcja-btc-nie-pizaa/>

```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;íýz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ā`šQ2:Ý.à
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)_ıÿÿ...~+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ö.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *...CA.gšY`bUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gh|q0·.Ō~(à9.¡
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybàè.ab*İÖñ?Lİ8Ä
00001000 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 GÜ.ã.ā.b\8M+ø..W
00001010 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 00 ŠLp+kã._~....
```

POWOLNY POCZĄTKOWY
ROZRUCH PROJEKTU



- ▶ 5 października 2009
 - ▶ 1 \$ = 1309 BTC
 - ▶ pierwszy, realny kurs wymiany Bitcoina ustalono na podstawie kosztu wydobycia, a nie na podstawie prawa popytu i podaży
- ▶ luty 2010 giełda Bitcoin Market
- ▶ giełda Mt. Gox.
 - ▶ 17 lipca 2010: 0.05 \$ = 1 BTC (1\$ = 20.00 BTC)
 - ▶ 18 lipca 2010: 0.09 \$ = 1 BTC (1\$ = 11.11 BTC)



PIERWSZE KURSY BTC

REACHABLE BITCOIN NODES

Updated: Thu May 23 21:37:05 2024 CEST

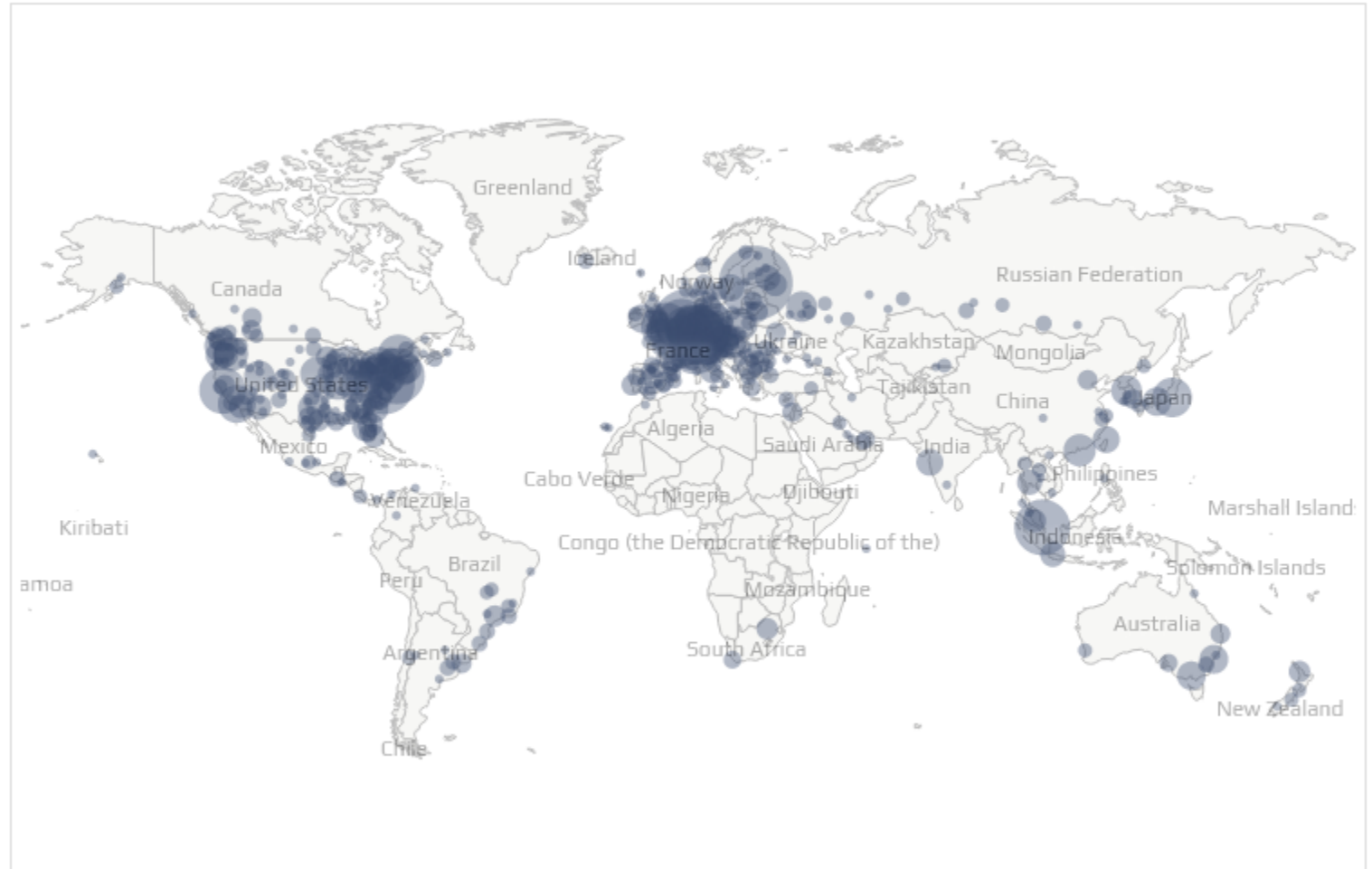
19318 NODES

[CHARTS](#)

IPv4: +4.4% / IPv6: -6.0% / .onion: +5.4%

Top 10 countries with their respective number of reachable nodes are as follows.

RANK	COUNTRY	NODES
1	n/a	12163 (62.96%)
2	United States	1760 (9.11%)
3	Germany	1747 (9.04%)
4	France	453 (2.34%)
5	Netherlands	330 (1.71%)
6	Finland	307 (1.59%)
7	Canada	286 (1.48%)
8	United Kingdom	216 (1.12%)
9	Japan	188 (0.97%)
10	India	187 (0.97%)



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

[LIVE MAP](#)

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEPkJEPeCh43BeKJLybLCWrDpN.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

VERIFYING THE TRANSACTION

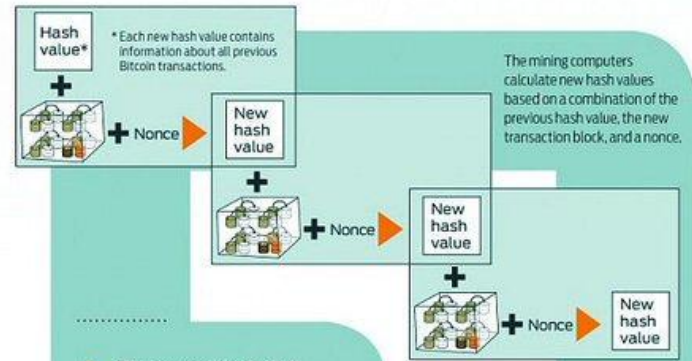
Gary, Garth, and Glenn are Bitcoin miners.

The miners' computers are set up to calculate cryptographic hash functions.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.



Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil → 6d0a 1899 086a... (56 more characters)

The root of all evil → 486c 6be4 6dde...

The root of all evil → b8db 7ee9 8392...

The root of all evil ??? → 0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

Nonces

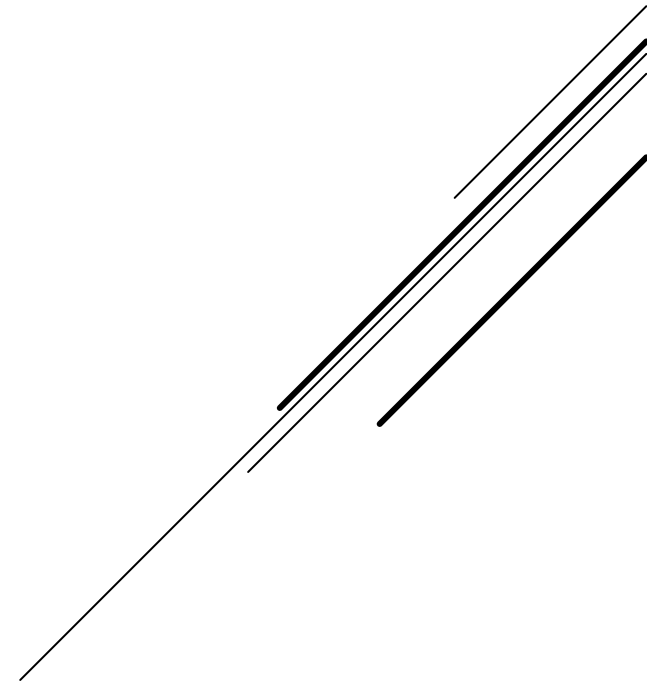
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

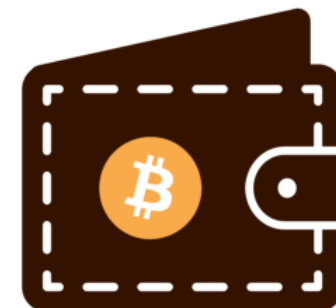
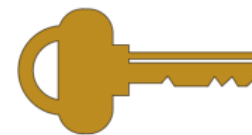
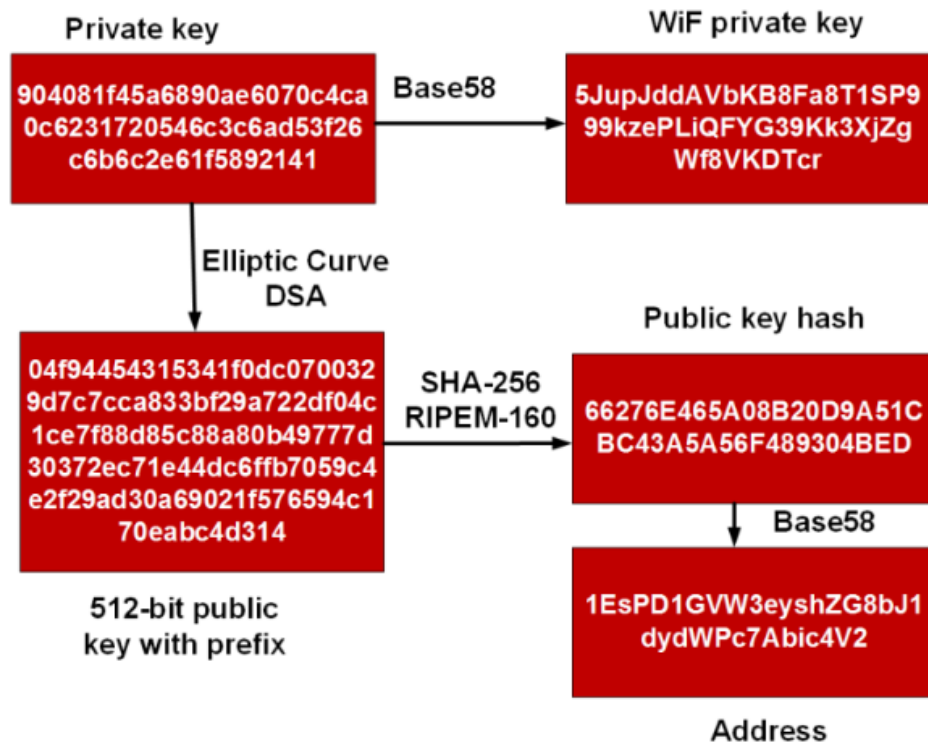
The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TWORZYMY ADRES BTC

Na przykład <https://www.bitaddress.org/>





klucz prywatny – pełen dostęp do środków

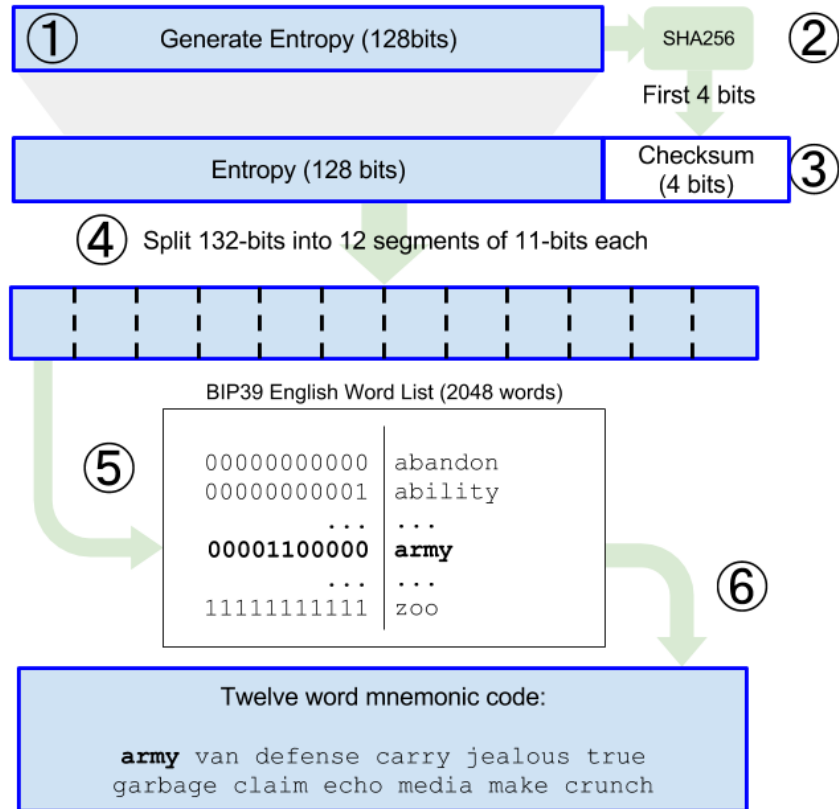
OD KLUCZA DO ADRESU

- ▶ Kod mnemoniczny (ang. seed *) to inna „forma zapamiętania” liczby losowej
 - ▶ liczba ta będzie wykorzystana do utworzenia klucza prywatnego **k**
- ▶ Kod mnemoniczny stanowi ciąg 12 - 24 wyrazów w danym języku
 - ▶ English 日本語 Español Français Italiano ...
- ▶ Standard BIP-39 zaproponowany przez producenta Trezor (powszechny)



A CO MA DO TEGO SEED?

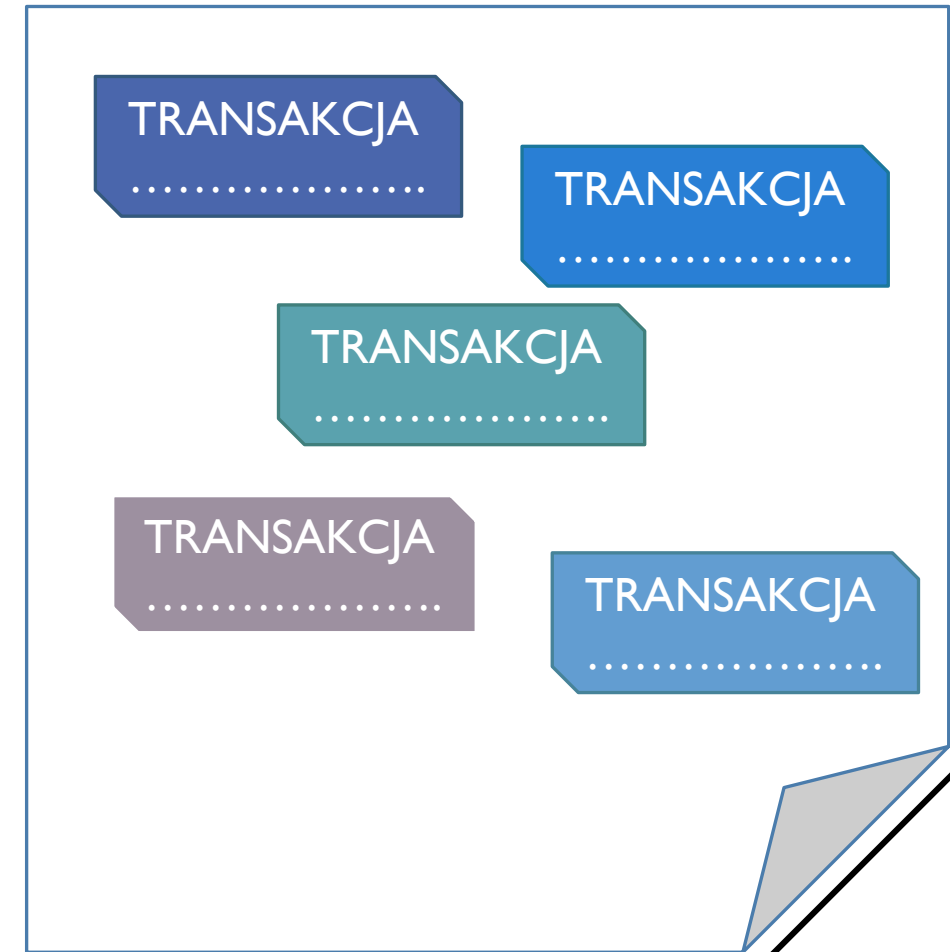
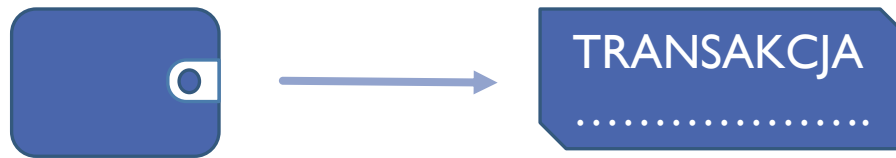
Mnemonic Words 128-bit entropy/12-word example



JAK JEST WYBIERANY KOD MNEMONICZNY

1	abandon	660	fame	2009	wild
2	ability	661	family	2010	will
3	able	662	famous	2011	win
4	about	663	fan	2012	window
5	above	664	fancy	2013	wine
6	absent	665	fantasy	2014	wing
7	absorb	666	farm	2015	wink
8	abstract	667	fashion	2016	winner
9	absurd	668	fat	2017	winter
10	abuse	669	fatal	2018	wire
11	access	670	father	2019	wisdom
12	accident	671	fatigue	2020	wise
13	account	672	fault	2021	wish
14	accuse	673	favorite	2022	witness
15	achieve	674	feature	2023	wolf
16	acid	675	february	2024	woman
17	acoustic	676	federal	2025	wonder
18	acquire	677	fee	2026	wood
19	across	678	feed	2027	wool
20	act	679	feel	2028	word
21	action	680	female	2029	work
22	actor	681	fence	2030	world
23	actress	682	festival	2031	worry
24	actual	683	fetch	2032	worth
25	adapt	684	fever	2033	wrap
26	add	685	few	2034	wreck
27	addict	686	fiber	2035	wrestle
28	address	687	fiction	2036	wrist
29	adjust	688	field	2037	write
30	admit	689	figure	2038	wrong
31	adult	690	file	2039	yard
32	advance	691	film	2040	year
33	advice	692	filter	2041	yellow
34	aerobic	693	final	2042	you
35	affair	694	find	2043	young
36	afford	695	fine	2044	youth
37	afraid	696	finger	2045	zebra
38	again	697	finish	2046	zero
39	age	698	fire	2047	zone
40	agent	699	firm	2048	zoo

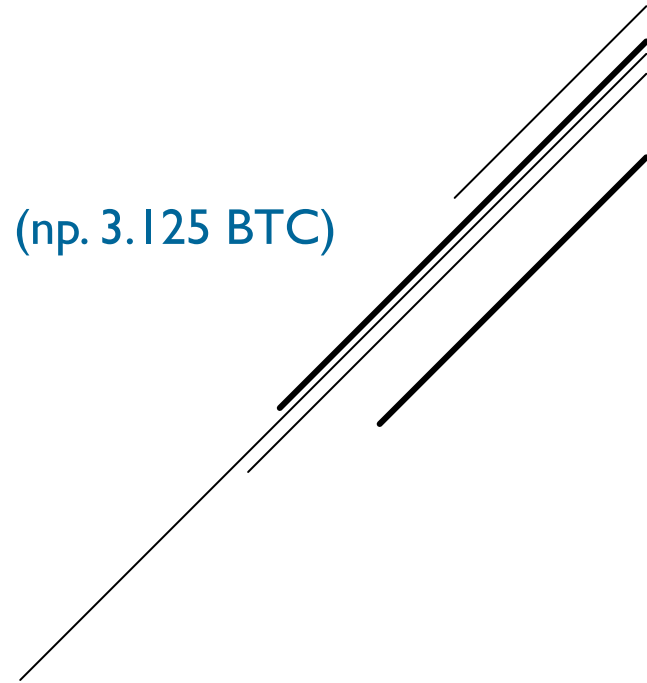
- ▶ Użytkownik tworzy nową transakcję
 - ▶ wykorzystuje do tego swój klucz prywatny
 - ▶ transakcja jest walidowana
- ▶ Transakcja ta trafia do mempool-a
 - ▶ miejsce, w którym wszystkie prawidłowe transakcje czekają na potwierdzenie



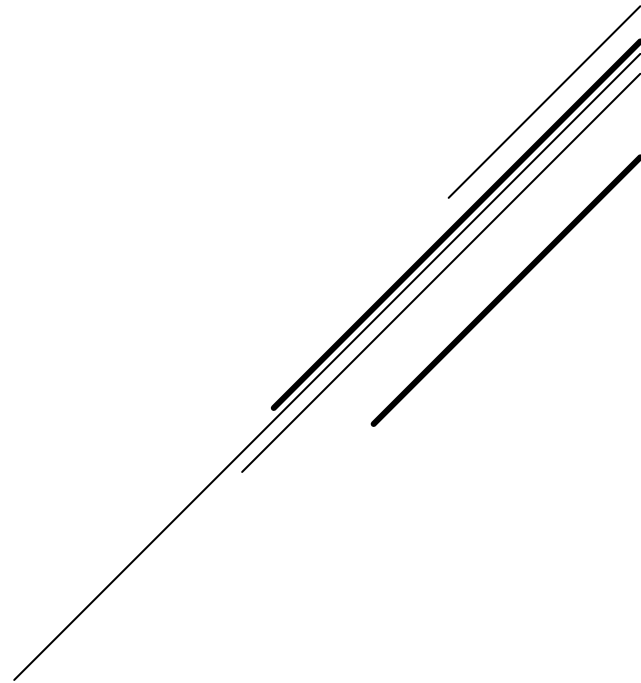
MEMPOOL

- ▶ „Górnik” wybiera z mempool-a transakcje
 - ▶ najczęściej te które posiadają najwyższą opłatę transakcyjną
 - ▶ ograniczony jest wielkością bloku danej kryptowaluty (np. 1MB dla BTC)
- ▶ Tworzy własny blok
- ▶ Poszukuje wartości losowej (*nonce*)
 - ▶ która w połączeniu z haszem wszystkich transakcji w bloku zaczyna się ciągiem 000..
- ▶ Jeśli znajdzie *nonce* to rozgłasza tę informację do pozostałych użytkowników
- ▶ Blok zostaje dodany do łańcucha bloków (*blockchain*)
- ▶ „Górnik” otrzymuje nagrodę w postaci nowo wydobytych jednostek kryptowaluty (np. 3.125 BTC)

Z MEMPOOL-A DO BLOCKCHAIN-A

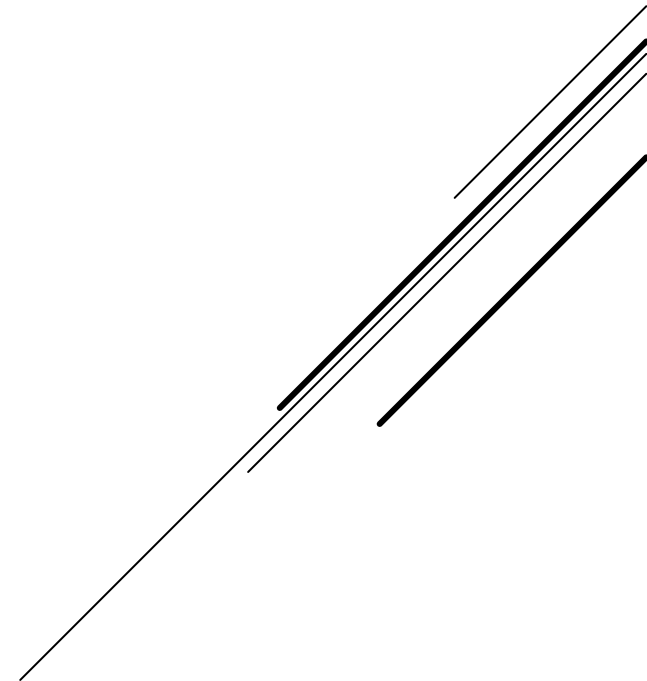


C. PSEUDOANONIMOWOŚĆ



- ▶ wszystkie zapisy w blockchainie dostępne do sprawdzenia przez każdego, wszystkie adresy użyte do transakcji oraz wszystkie transakcje są jawne
- ▶ pseudoanonimowość
 - ▶ zapewnienie jawności transakcji
 - ▶ nie wiązanie jej z konkretną osobą
- ▶ de-anonimizacja (konkretnej osoby)
 - ▶ „łączenie” transakcji z giełdami, kantorami
 - ▶ badania z użyciem analizy heurystycznej

PSEUDOANONIMOWOŚĆ



Transakcja Zobacz informacje o transakcji bitcoin

63c5f2ec7d5a88265e26f687a532dfe5b5071c9971beb2decddab135cb4696d2

13X8swZWP54N6C9La1M9QzfPcSwwUNUnbg



1JYQkbrMgeHHydNzMCaJe2VtpwmSjMW7wf
15zdGLs5u7Z5z2j16qJvpjwsRn1wMPJBnG

0.0198 BTC
0.00656749 BTC

1 Potwierdzenia

0.02636749 BTC

Podsumowanie

Rozmiar 225 (Bajtów)
Waga 900
Czas otrzymania 2018-04-04 07:52:55

Zawarta w blokach [516562](#) (2018-04-04 07:55:21 + 2 minut)

Potwierzeń 1 Potwierzeń

Wizualizacja [Zobacz wykres drzewa](#)

Przychody i wyjścia

Razem przychodów 0.02736749 BTC

Razem wychodzących 0.02636749 BTC

Oplaty 0.001 BTC

Oplata za bajt 444.444 sat/B

Oplata za jednostkę wagi 111.111 sat/WU

Szacunkowa ilość BTC w transakcji 0.00656749 BTC

Skrypty [Pokaż skrypty & coinbase](#)

Blok #516562

Podsumowanie

Liczba Transakcji 2520

Razem wychodzących 11,182.21997248 BTC

BLOCKCHAIN

WALLET

DATA

API

ABOUT

Czas 2018-04-04 07:55:21

Czas otrzymania 2018-04-04 07:55:21

Przekazany przez [BTC.com](#)

Trudność 3,511,060,552,899.72

Bitów 391129783

Rozmiar 1256.8 kB

Waga 3992.932 KWU

Wersja 0x20000000

Nonce 4174425017

Nagroda za blok 12.5 BTC

Transakcje

511ab4f13db7d4a41f70dce09e54436b1d4c4c4225c2d6da9e8d3628a551bd0d

Brak wejść (nowe monety wygenerowane)



1C1m
Nie m

63c5f2ec7d5a88265e26f687a532dfe5b5071c9971beb2decddab135cb4696d2

13X8swZWP54N6C9La1M9QzfPcSwwUNUnbg



1JYQ
15zd

BLOK I TRANSAKCJA

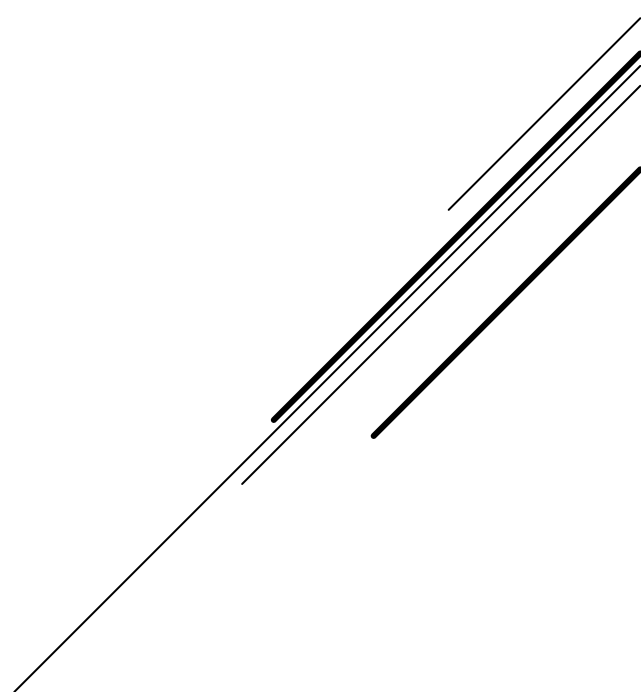
- ▶ Tylko niezerowa liczba bitcoinów może być przesyłana z jednego adresu na drugi.
- ▶ Każda transakcja składa się z dwóch stron: wejściowej i wyjściowej.
- ▶ Adresy znajdujące się po stronie wejściowej, zwane dalej w pracy adresami wejściowymi, muszą posiadać wystarczającą liczbę bitcoinów dla danej transakcji. Nie ma możliwości przesłania z danego adresu większej liczby bitcoinów niż jest w jego posiadaniu. **Cała kwota znajdująca się na adresach wejściowych musi zostać wydana w pojedynczej transakcji.** Przy czym po stronie wyjściowej mogą znajdować się te same adresy co po stronie wejściowej.
- ▶ Liczba bitcoinów znajdujących się po stronie wejściowej transakcji musi być równa liczbie bitcoinów znajdujących się po stronie wyjściowej transakcji powiększonej o ewentualną opłatę transakcyjną.

TRANSAKCJE – ZASADY

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b	→ 1A1zP1eP5QGefi... (Genesis of Bitcoin ↗)	50 BTC
		50 BTC
4624ef0a9fd63c40ca6f789ad34eee5f1ac92a23490596192f7a7286c51a2cd7	→ 1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB Nie można dekodować adresu wyjściowego	12.77401803 BTC 0 BTC
	9 Potwierdzenia	12.77401803 BTC



RODZAJE TRANSAKCJI 0 → 1



281b0e73b30f2bbb4f1859ed432cceb9e1431418794b27247f72ea834da73268

16Nj2vwbcidN1miG5qFvY2iUSmeZ1cKTzy



1KejHZHms744ua6rcFAfo211c3HS71JhyS

0.01097309 BTC

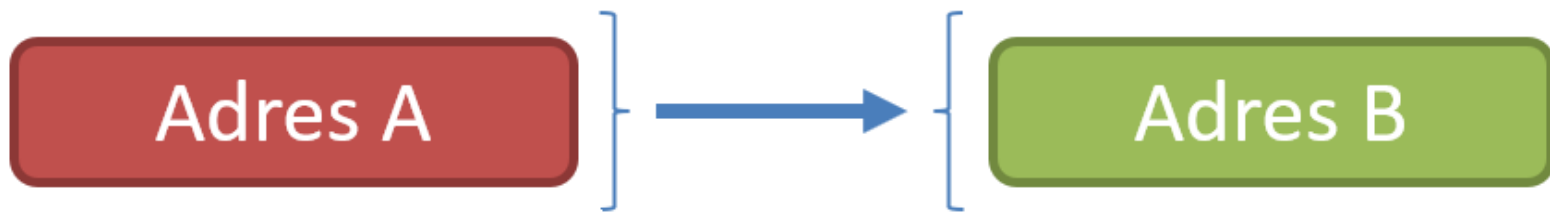
0.01097309 BTC

Podsumowanie

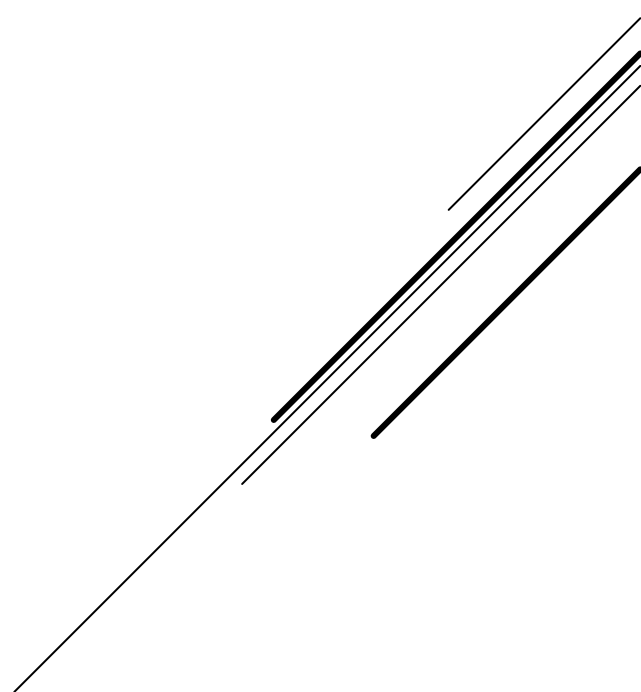
Rozmiar	223 (Bajtów)
Waga	892
Czas otrzymania	2016-05-15 20:16:39

Przychody i wyjścia

Razem przychodów	0.01098 BTC
Razem wychodzących	0.01097309 BTC
Oplaty	0.00000691 BTC



RODZAJE TRANSAKCJI | → |



3c6409ecb159df64d59a55b9368a40787b4dd7eed721a11593c1b04e6e5328a5

1CuBgumLwcR2gSac6nW23uWuhMqVs6TwUg



1KLpmhwuiF4JhPJ8e7p6nFFbeChCzirSq8
1KYMJ5T5YJKLN7LYgs9Rrzj7FCvqWPjq6j

89.38738 BTC

0.18 BTC

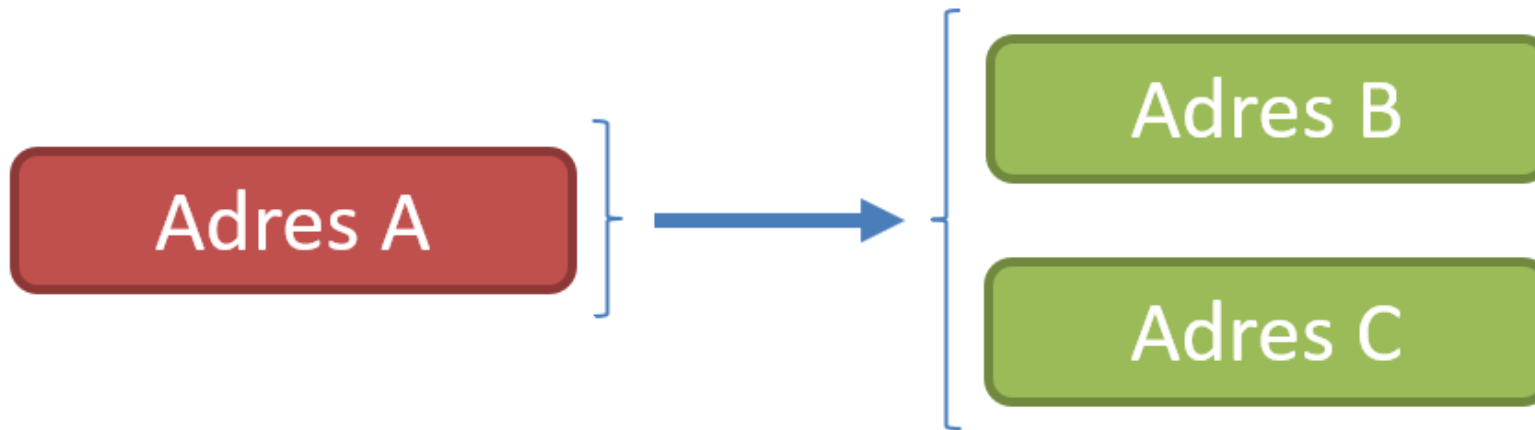
89.56738 BTC

Podsumowanie

Rozmiar	226 (Bajtów)
Waga	904
Czas otrzymania	2017-01-27 13:30:45

Przychody i wyścia

Razem przychodów	89.5676286 BTC
Razem wychodzących	89.56738 BTC
Opłaty	0.0002486 BTC



RODZAJE TRANSAKCJI 1 → 2

3b978e586018d51de04e1a2624081bf0f9679b40af5aada49a903607fc3a052b

1KYMJ5T5YJkLN7LYgs9Rrzj7FCvqWPjq6j
1MUqFqUZsB6BKppMPRkah5cnQYp77ZAwzn
1Lfkzuf6Hr86wRWctWBSa2vefqWKKZmQJ5
1HgEKpzKzQ98EfGALcUF32Ngn4aAcivG1A
1LhCu8jh8AVLEm9qETAQBx3PHqJNhDnmvQ
1MRsGAVUJnm1PkxhuwVkJZqmpKG2ec6EFLa
1D8k5b4b4ZCyBf1WpaRdSswQxNnXgu1MCM
1Je2XMNhnxz5W3q8cuYE52Cx7GHzwG3VJf



1Pm5mYudt5jWYP29AvM6g9fDcagidGR7kR

4.63 BTC

4.63 BTC

Podsumowanie

Rozmiar	1668 (Bajtów)
Waga	6672
Czas otrzymania	2017-01-31 11:42:24

Przychody i wyścia

Razem przychodów	4.6317288 BTC
Razem wychodzących	4.63 BTC
Oplaty	0.0017288 BTC

RODZAJE TRANSAKCJI N → I

4410c0c086eaa45365b7e6ca35953539304949c90e01acf8a96d92dff35cb7d5

19knN1QLjBytwr5FV5eVCgSAfUwuRqmU7o
1PVMtEbbR5twrXBpTRtmZEZ7VrzKYA8tbn
1GkpT5sLP4DyQki8ZfBqzLYK2U9pQCbpvr
1JLicgbLWiyYJiDbhQfUFwQKfQPxs4dkD
14fMCHMNV53wkak1jv3dEb9erCWtSRiByx
1PE51qiV8m3KWZuDheBvzcWCQNfzpenuv
1D4o8ECXFckiFkSDxvFi2NcQX7KWpSLUbG



1PxEEisNJDc3uAe75vbAsb4jkUyV8QhNYG
19zJb3sg78aHv1Jg9B5aVjUwSQeWQ6kvdg

1.40111321 BTC

0.01000463 BTC

1.41111784 BTC

Podsumowanie

Rozmiar	1175 (Bajtów)
Waga	4700
Czas otrzymania	2016-07-09 09:28:09

Przychody i wyjęcia

Razem przychodów	1.41353384 BTC
Razem wychodzących	1.41111784 BTC
Oplaty	0.002416 BTC

RODZAJE TRANSAKCJI N → 2

19NaxUoUWEJLZXzwnahi9wjf16HoUjWB6o
 1BZoJ5A8DZY2wk2dkrFCYcNp3m4wHpoggM
 13phPJ4a8yjo7uYqBEqNpPCw3YF4yYRvj
 1CPMLny76P1Myk9B78hJBHa1t8YSWFYsGM
 112ch8mPU9r4R7gtTvPUU7UgR1GR2bEUoh
 12u3DDXzR4Q9m5uUrPYxpucJ4eoYq5rdDi
 1pgJ4AoUrgroiFgL8zoSiX8kuZQ4Vhsq
 1C66sXCXGa7uA2PYkiTfAZf5aG8C5CyejP
 1JYqeUrjcP3R2PiWq2cazDfjNK6Jif9zG
 19emG7L4Cu53229H7S44SpevtHtGhWyseT
 1DYjKcvEWbuSsMKVuopYvpembYcnVcstoB
 1HmZ9HQX38edAbpkT98TdG2jVmkzEtMmpE
 1K8K6Agh5TX3y6wrf1g1i3WL8UAbebuEEP
 1Mp5RFhhWCwjKapnQfgJreSgJ4CChX4Xa
 1GbFwTPqcdfzDku5431UWze4RKjC77NVJ7
 1KjJtuN4znGkd77bwcBTuWzHCZpY5WPzYx
 15wsVKy11BScmrBhgNFYwWdMir7XdALfkc
 1KBPLnSaLhLgSxjmDwEspjiL7ZHjFDajNH
 1Nm7995VV54mzUp7K7VN2enNP5yVAF4BWq
 13SGQp1MR1otMRJi4yGMRRpQRz1mtpxUQA
 1GYYTHDjyG8C7Dx4r9PuxEMTyTmxCd317X



1pKNa39SaGzjv2B3PhWTA62Pku1XUHV9d 1.683572 BTC
 1EWkz13EfEHFcEmu52MMiMjhcV5GfECTCE 8.364422 BTC
 19f2WKJ2ibfG1Rzp9RNaURDiciL6PKq7xF 1.091 BTC
 1MaKPepS4vPxn5n4TGpkcTwosMG5oPcwhZ 1.10550838 BTC
 12NW2eWA95a6bjuDmpbJj4LhbcwpyDScav 7.021222 BTC
 15BEVbxtYT8AQTZe6gbWyxeQDoEHZnyghZ 1.11068017 BTC
 1JGNawQRqmngzu2pfr2t3K3pY82s5CbTqw 1.019 BTC
 15cXikA1U6gWnoXsQGKVh98sTvQbYRcuAZ 1.144 BTC
 1MvYxmpag6xwrPKZoraKAjvcahfnhx44 1.0884 BTC
 1CoN7sh1gyCqkH9KJzVX6oFQm7wa6L6kXB 0.993 BTC
 1JbwR7Nu9B1rTcdppqkgum9JVSmlLiakuWc 1.1471 BTC
 1JYqeUrjcP3R2PiWq2cazDfjNK6Jif9zG 0.15417011 BTC
 1Eyj7mh4wicN3TddTvyoHH5C2CKWsRM4uc 1.07665831 BTC
 1KdvDgrk9rjNsWnTmSFkC5oXgAn58rGvmn 1.04840443 BTC
 12uK2YyVG4urGmarZEfLVYSnsFXr1Ujtgf 1.11200831 BTC
 19xUAF4u5SafZrncHMC9FBFKzMyXSehaxp 1.119581 BTC
 1BKirpHM9xwMLrgjiUTox5BSzKujxUanFF 1.040242 BTC
 15DMH9GpNFxbSdLxdMHngcY2xf3qYn6dch 1.0477404 BTC
 1C34GFcC4Xe1rU7Q6298zP8FL3WBD3MQgU 0.9835 BTC
 13eRtad7LBwHbTJZ11XMa7sit3ZHwpRT1U 1.083597 BTC
 1PXnwjGa5XNrFzZYhyJWkXU54AAvtjZ99a 1.13 BTC

35.56380611 BTC

Podsumowanie

Rozmiar 4219 (Bajtów)
 Waga 16876
 Czas otrzymania 2014-10-05 05:28:51

Przychody i wyjęcia

Razem przychodów 35.56430611 BTC
 Razem wychodzących 35.56380611 BTC
 Opłaty 0.0005 BTC

7957151ab2ac8ad51a6117c0e56baf4e8a769f93a603b9ea8e2b2f66c5b37536

1GXerksFNbckEmQBt7TT4Vu97hRZNQVzna



1EHRiH14C7ojKAX7H3AWxmXHQxGrizQJwa
1KuuHVAbJSnfkYf93wmUf1WJUQhFx2Dntn
1Bs4F9sBNeTnV6EE9jjq3DoYn6Vq1LR4Yz
1BBnMCFjf5KijJwRGzZdVdvrX8mxMKx9Y2

0.01 BTC

0.74794977 BTC

0.01 BTC

0.01 BTC

0.77794977 BTC

Podsumowanie

Rozmiar 294 (Bajtów)

Waga 1176

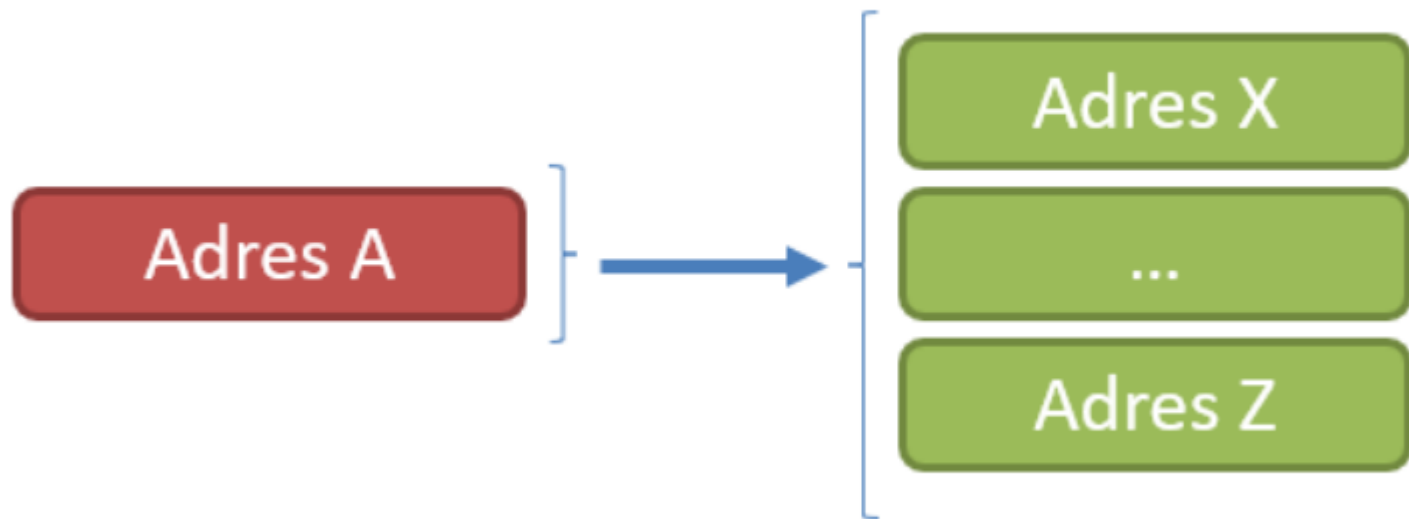
Czas otrzymania 2016-07-09 23:26:37

Przychody i wyjścia

Razem przychodów 0.77839253 BTC

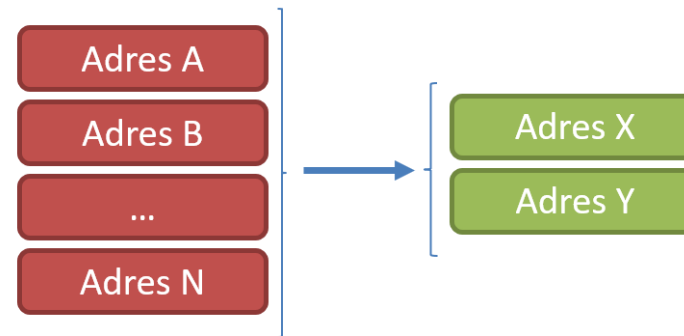
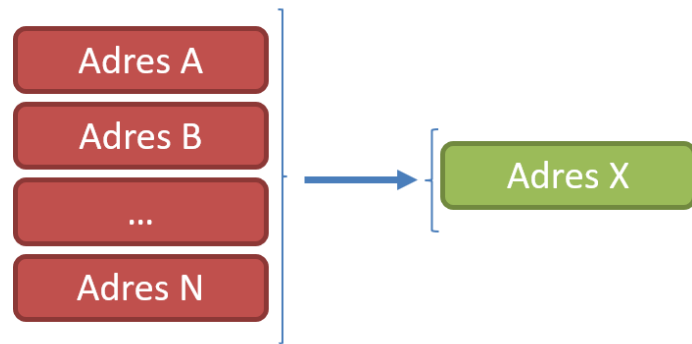
Razem wychodzących 0.77794977 BTC

Oplaty 0.00044276 BTC



RODZAJE TRANSAKCJI I → M

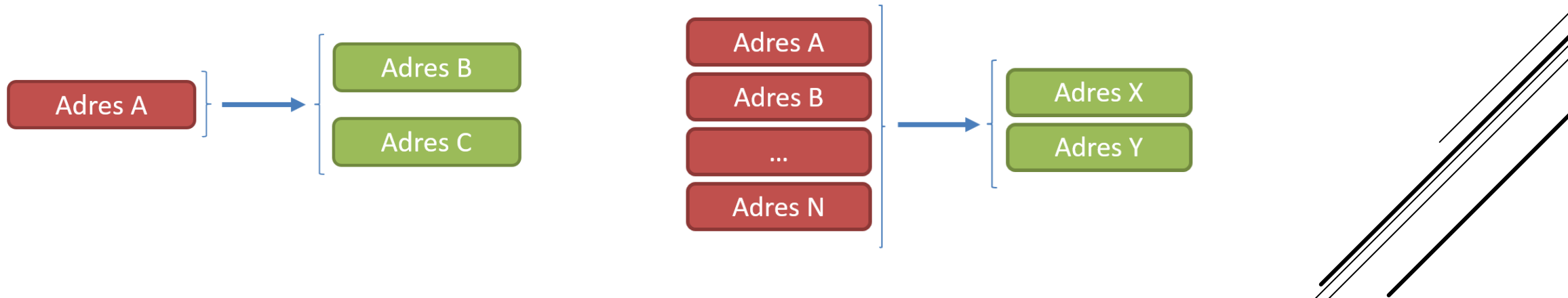
- ▶ Jeśli dwa lub większa liczba adresów wejściowych wymagających użycia pojedynczego klucza prywatnego wchodzi w skład pojedynczej transakcji to są one kontrolowane przez ten sam podmiot.



HEURYSTYKA I

Heurystyka - metoda znajdowania rozwiązań, dla której nie ma gwarancji znalezienia rozwiązania prawidłowego

- ▶ Jeśli transakcja składa się z dwóch adresów wyjściowych to jeden z nich (zwany adresem reszty) kontrolowany jest przez ten sam podmiot co adres(y) wejściowe
 - ▶ tylko który?

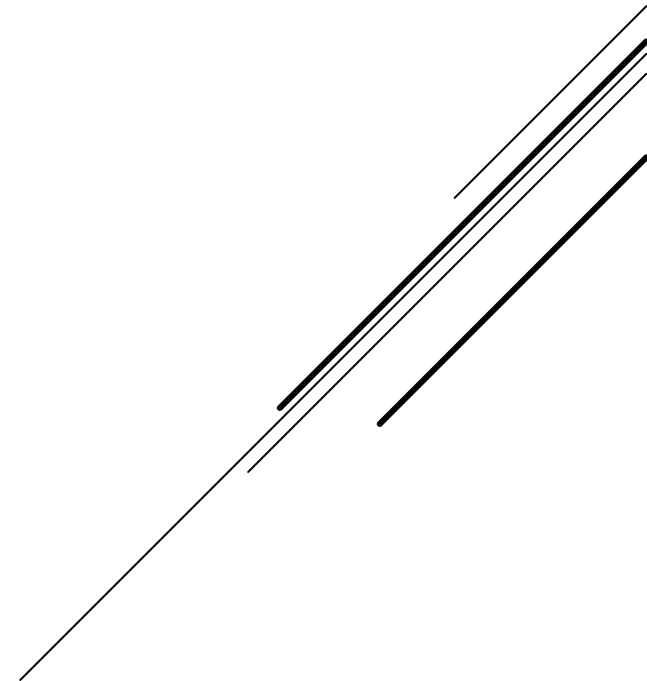


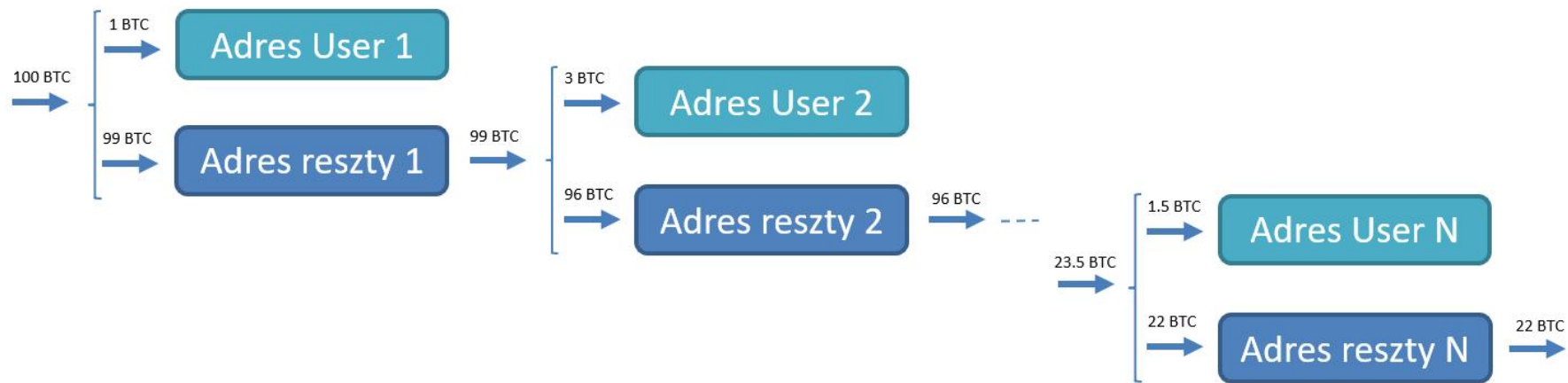
HEURYSTYKA 2

- ▶ sprawdzenie czy jeden z adresów nigdy wcześniej nie występował z łańcuchu bloków
 - ▶ jeśli tak, to można z dużym prawdopodobieństwem założyć, iż jest to właśnie adres reszty, gdyż wiele portfeli bitcoinowych działa właśnie w ten sposób – tworzy nowy adres dla kwoty stanowiącej resztę transakcji

HEURYSTYKA 2

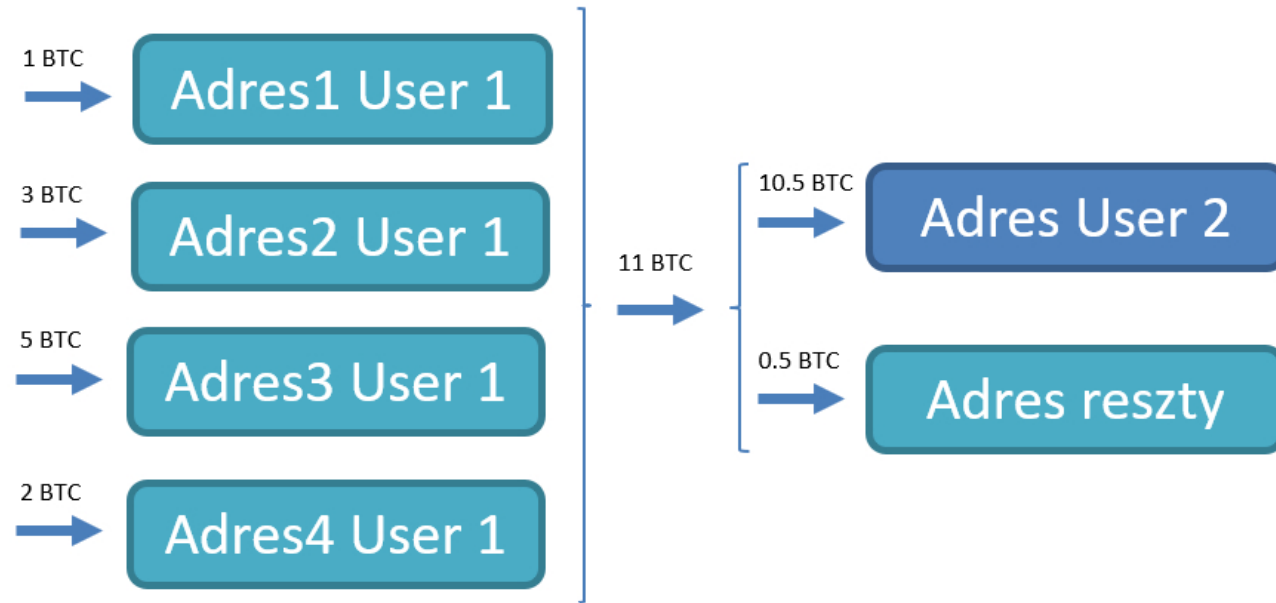
ADRES RESZTY – SCENARIUSZ I





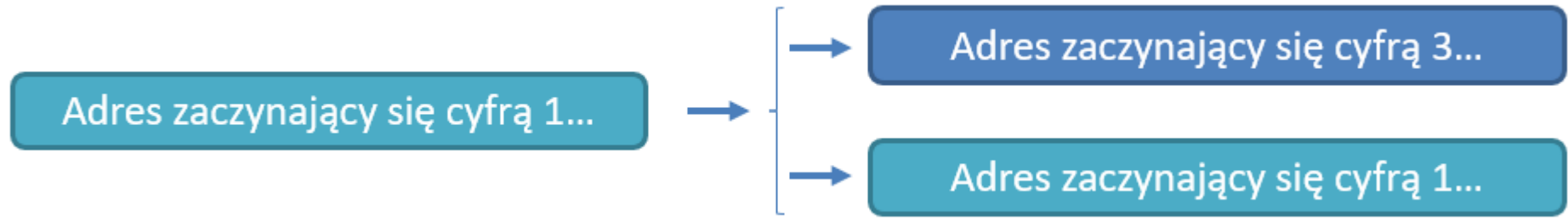
HEURYSTYKA 2

ADRES RESZTY – SCENARIUSZ 2



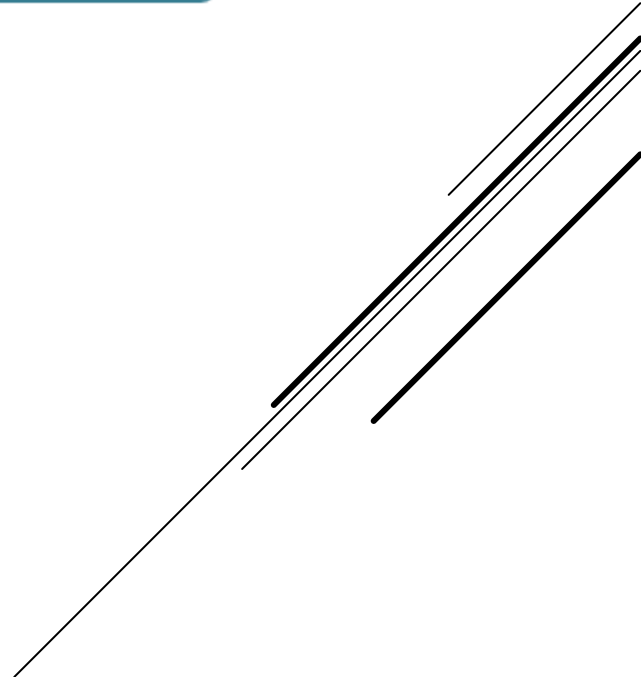
HEURYSTYKA 2

ADRES RESZTY – SCENARIUSZ 3



HEURYSTYKA 2

ADRES RESZTY – SCENARIUSZ 4



- ▶ jeden z najpopularniejszych altcoin-ów (alternative coin)
- ▶ data powstania: 2015
- ▶ autor: Vitalik Buterin (Rosja)
- ▶ model: proof-of-work do 15.09.2022, przejście na proof-of-stake
- ▶ schemat: bazujący na aktualnym saldzie koncie (ang. Account Based)
- ▶ maksymalna liczba jednostek waluty: brak
- ▶ więcej niż kryptowaluta:
 - ▶ kontrakty, tokeny, crowdfunding

ETHEREUM [ETH]



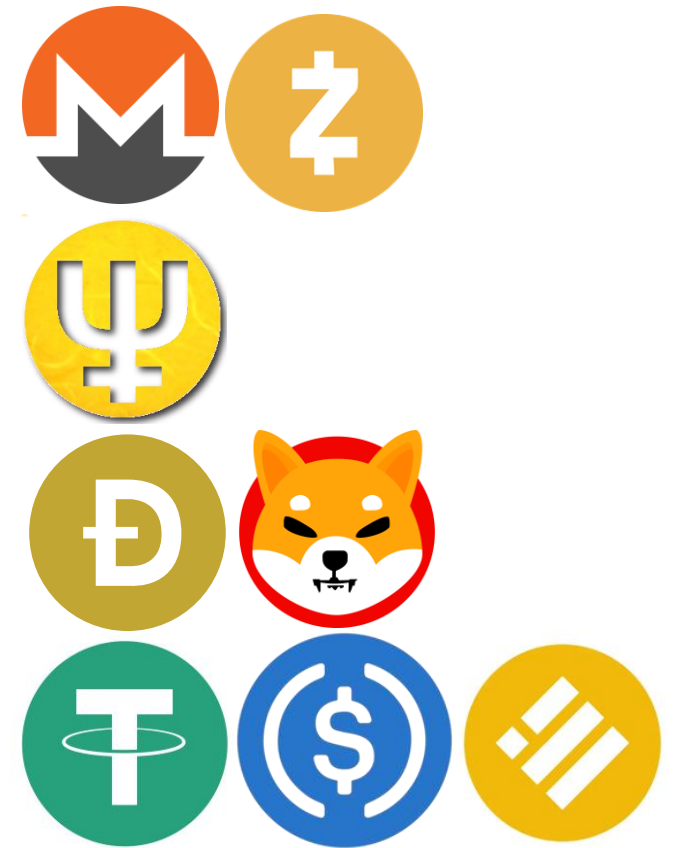
- ▶ Proof of Work (PoW) - dowód pracy:
 - ▶ wydobywania, kopanie (wykonywanie obliczeń)
 - ▶ BTC, ETH (do 2022), ...
- ▶ Proof of Stake (PoS) - dowód stawki
 - ▶ stakowanie (zamrożenie pewnej ilości danej kryptowaluty)
 - ▶ BNB (Binance Coin), TRON, ...
- ▶ Proof of Space (PoS) – dowód miejsca
 - ▶ farmienie (przeznaczanie przestrzeni dyskowej)
 - ▶ CHIA, SIA, ...
- ▶ ...



METODY OSIĄGANIA KONSENSUSU

- ▶ Anonimowość: Monero, Zcash, ...
- ▶ Pożyteczne: Primecoin, ...
- ▶ Memcoiny: Dogecoin, Shiba Inu, ...
- ▶ Stablecoiny: Tether (USDT), USD Coin (USDC), Binance USD (BUSD), ...
- ▶ Waluty banków centralnych (CBDC)

- ▶ Ponad **13 tysięcy** projektów
 - ▶ https://www.coinlore.com/all_coins



INNE KRYPTOWALUTY

Stablecoin – kryptowaluta powiązana na stałe z jakimś aktywem, np. USD, EUR

- A. Zasada działania kryptowalut, łańcuch bloków
- B. Klucze, adresy, transakcje
- C. Pseudoanonimowość

PYTANIA?

