“ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC”

Arthur C. Clarke

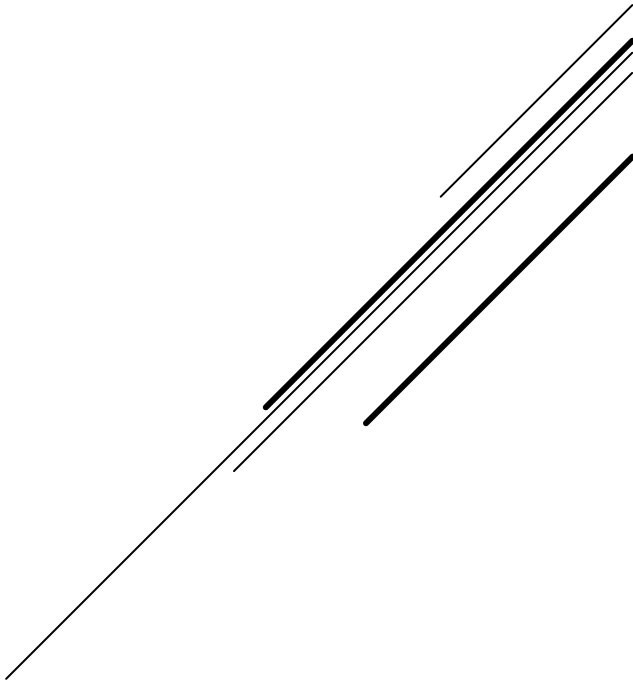
TEORIA

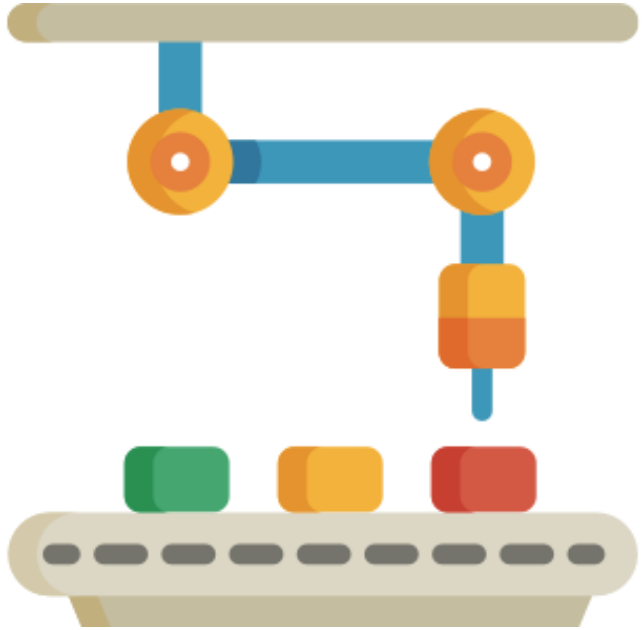
dr inż. Przemysław RODWALD

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

PLAN PREZENTACJI

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





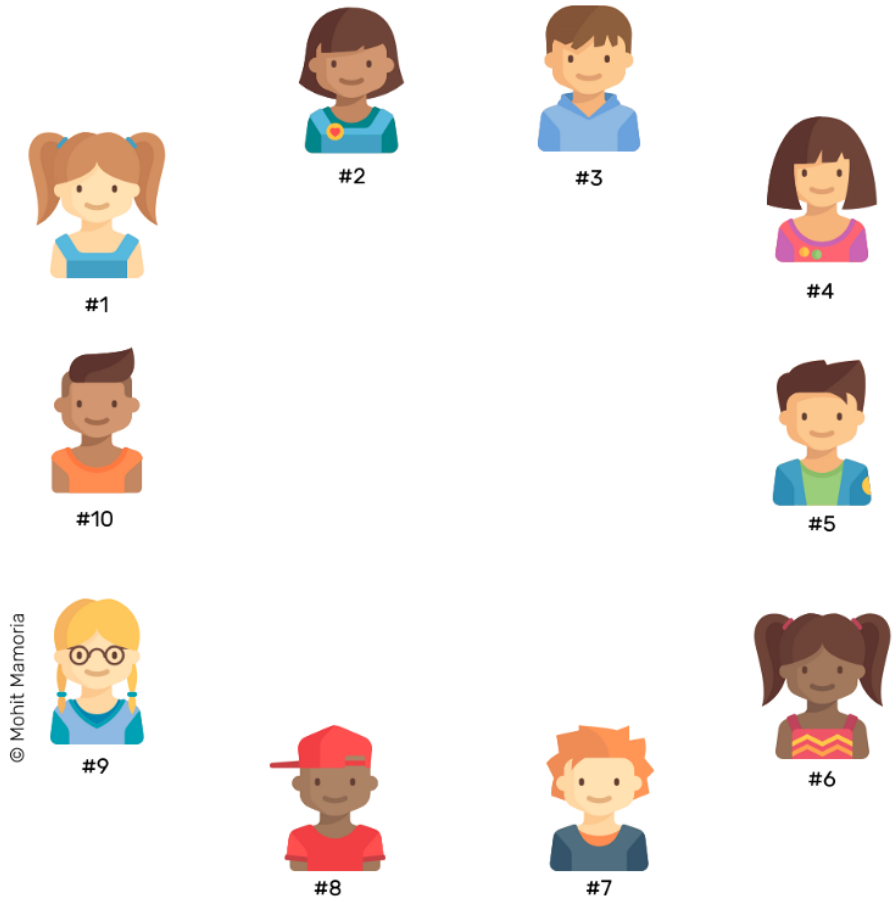
Na podstawie:

- *https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348*

A. „BLOCKCHAIN” NAJPROŚCIEJ

- załóżmy, 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

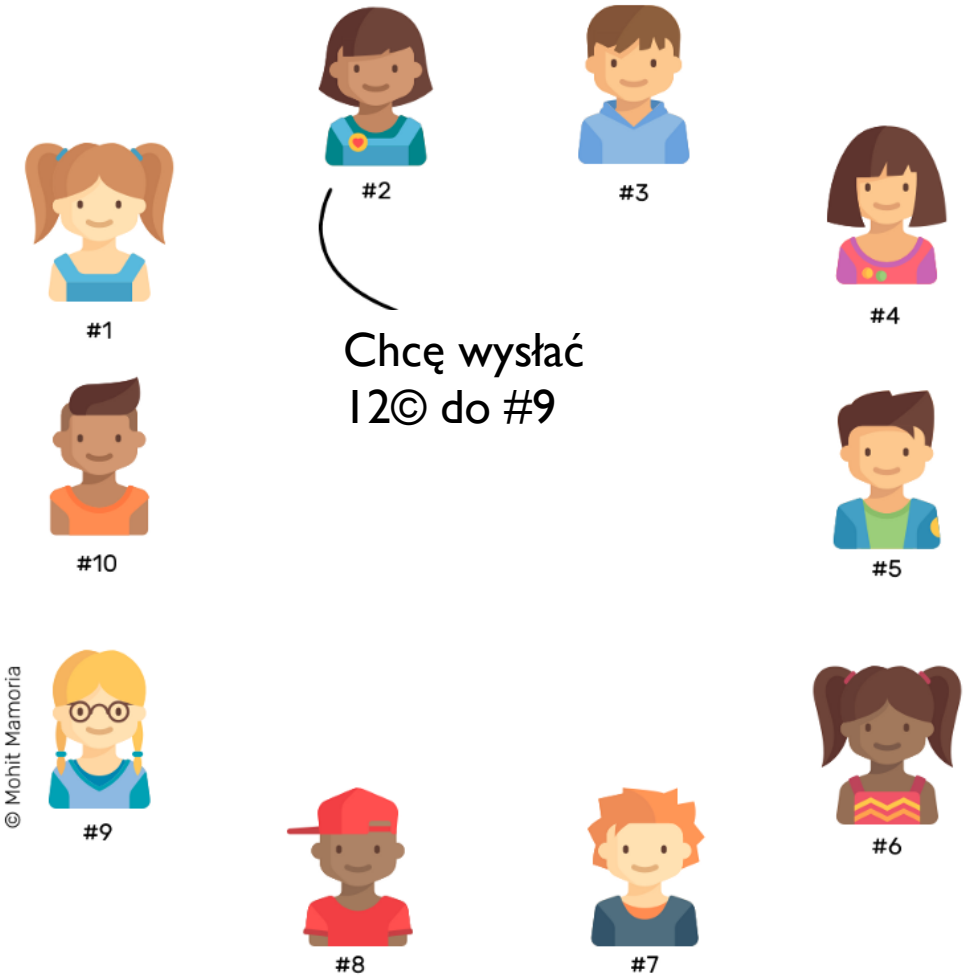


- każdy na początek ma pusty segregator
- w miarę jak będą dokonywane transakcje każda z osób będzie do swojego segregatora dodawać kolejne numerowane kartki
- ten segregator (uporządkowany zbiór kartek) będzie tworzył rejestr z zapisem wszystkich transakcji

1. PUSTY SEGREGATOR

- Każdy weźmie czystą kartę i długopis i przygotuje 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 #
    - jeśli tak, każdy zapisuje, że doszło do takiej transakcji
    - jeśli nie odrzuca transakcję

© - „nasz_coin” – waluta obowiązując w tym systemie

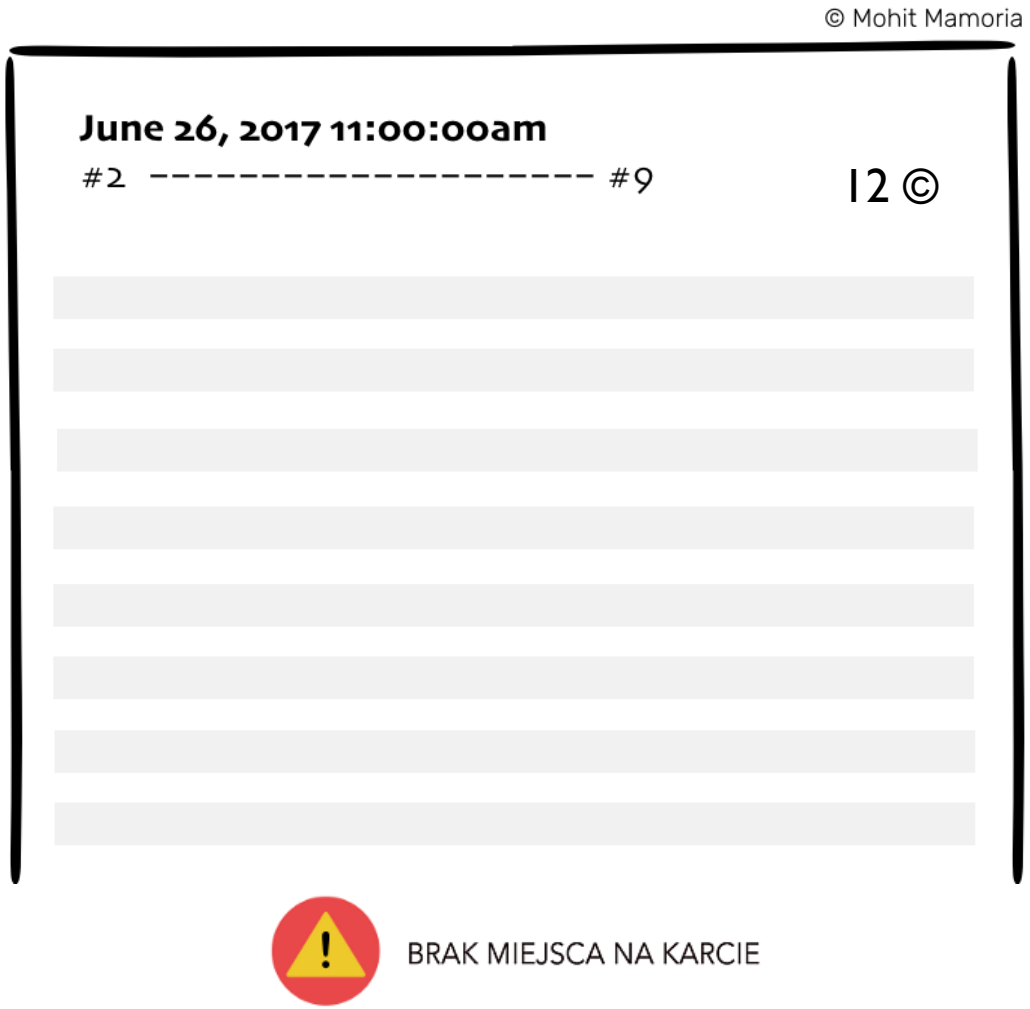


2. TRANSAKCJA

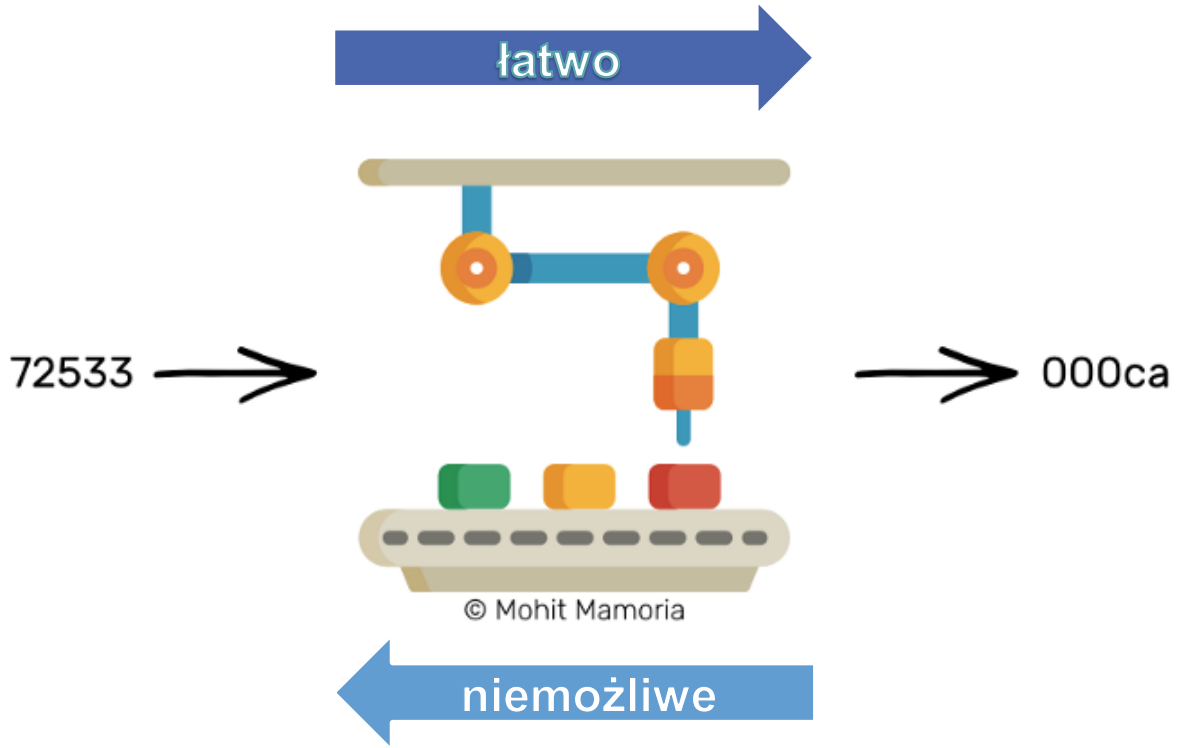
Pytanie: Czy wszyscy widzą transakcje innych użytkowników?

- 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

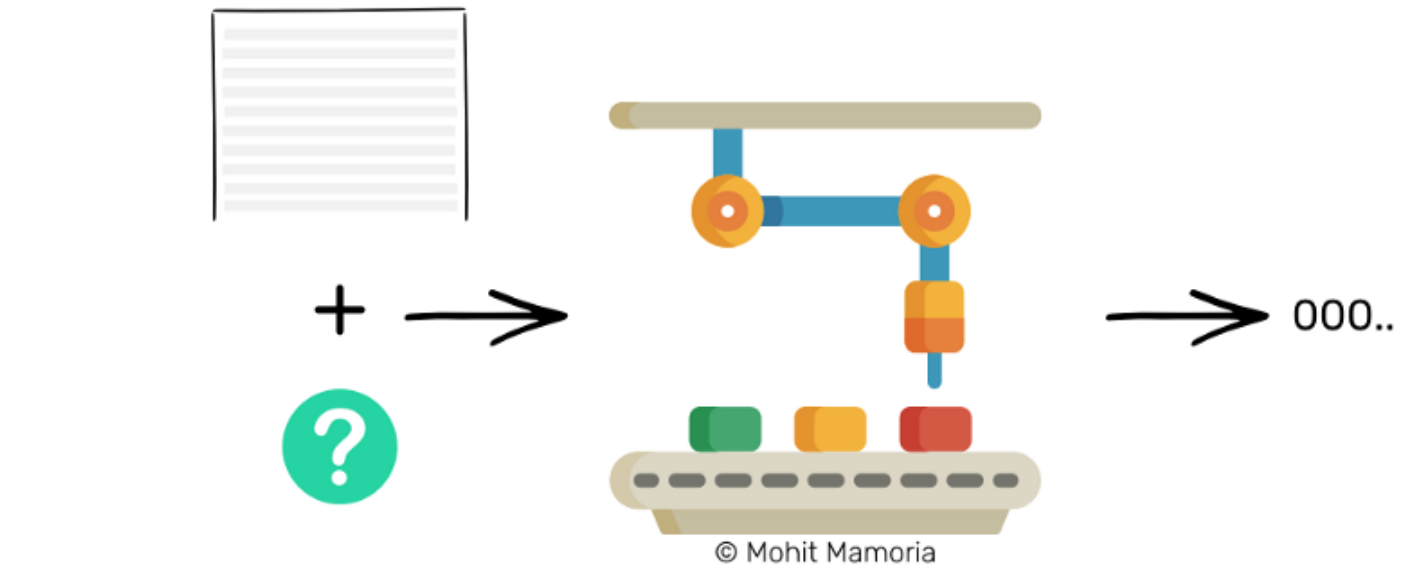


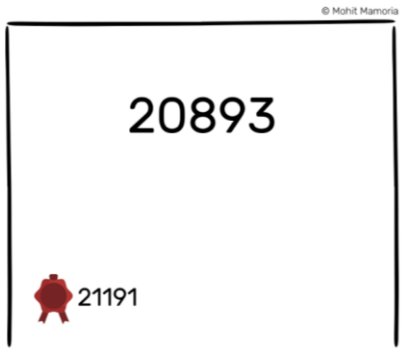
„MAGICZNA MASZYNA” CZYLI KRYPTOGRAFICZNA FUNKCJA SKRÓTU



.....

4. ZAPIECZĘTOWANIE KARKI



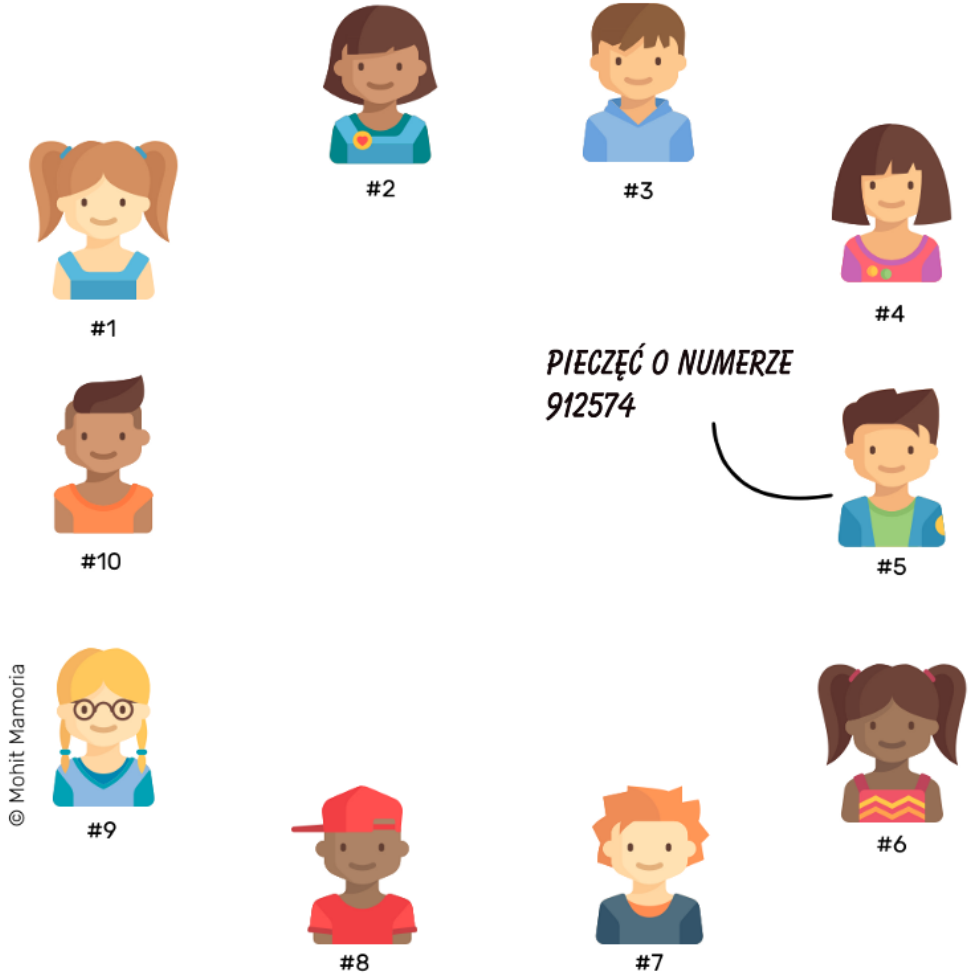


pieczęć to tzw. „proof of work”
- dowód na to, że podjęto trud związany z jej wyliczeniem

- 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 ja od innego użytkownika sieci.

Pieczęć którą wybierze większość uczestników sieci, będzie obowiązująca.

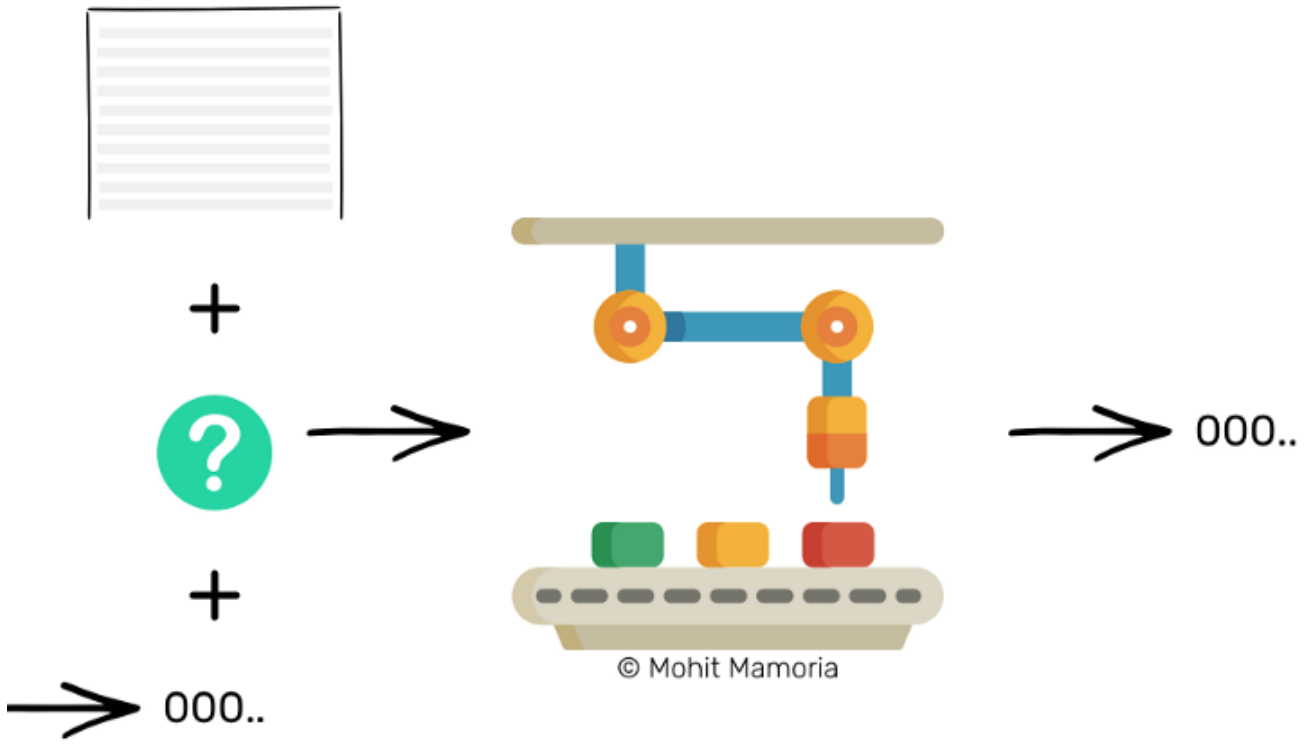
5. PIECZĘTOWANIE



PIECZĘTOWANIE - NAGRODA

- 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

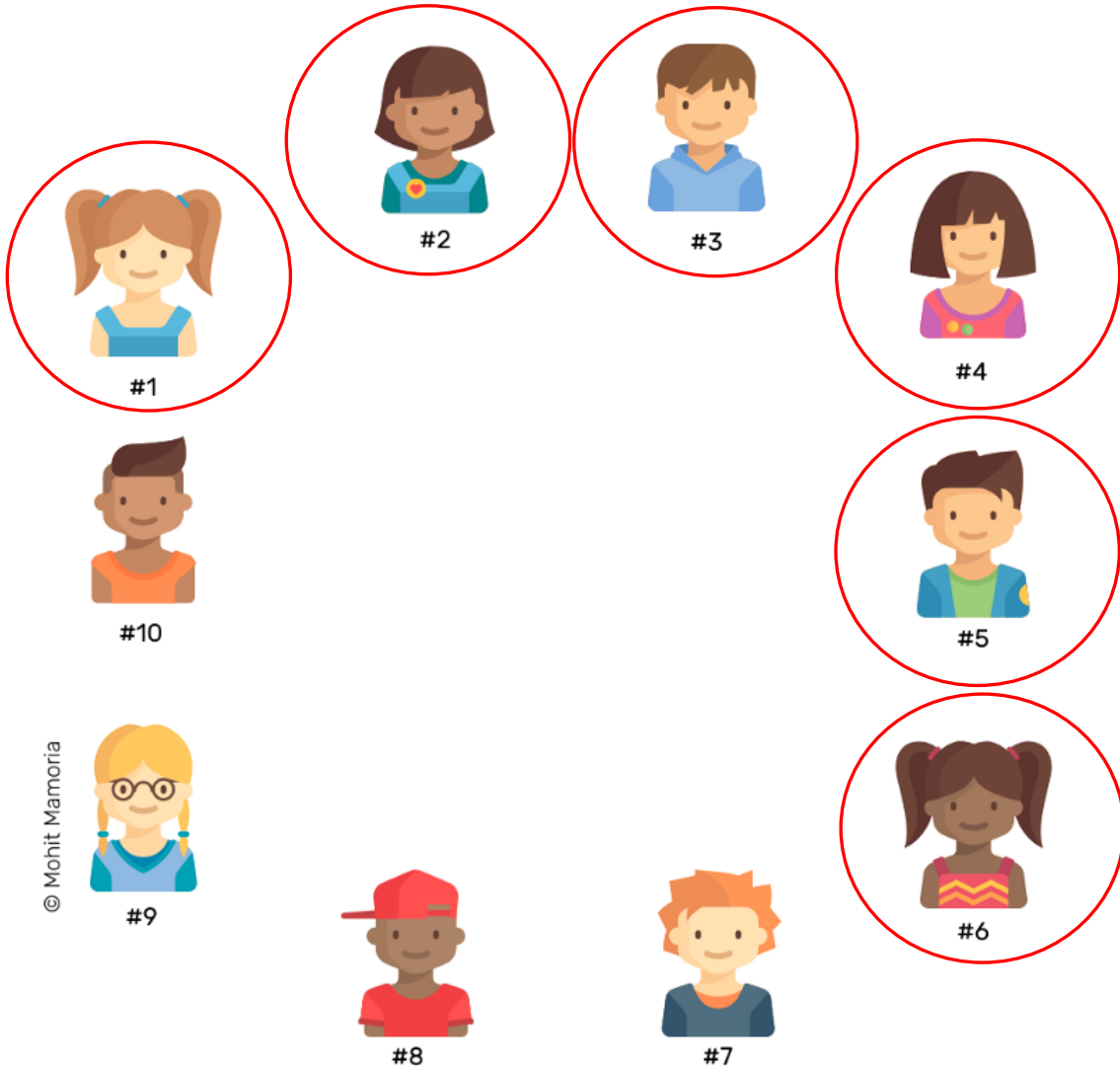
OCHRONA PRZED PODMIANĄ KART



- **atak 51%**

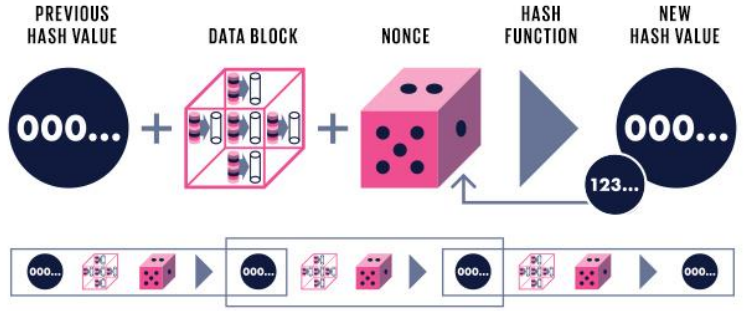
JAKIEŚ WADY?

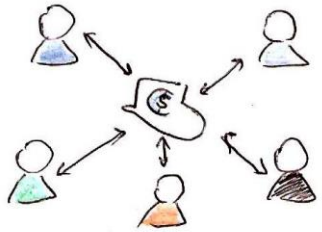
oszust

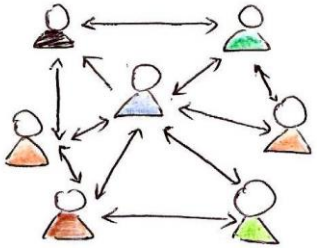


MECHANIZM DZIAŁANIA BLOCKCHAIN-A

- 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

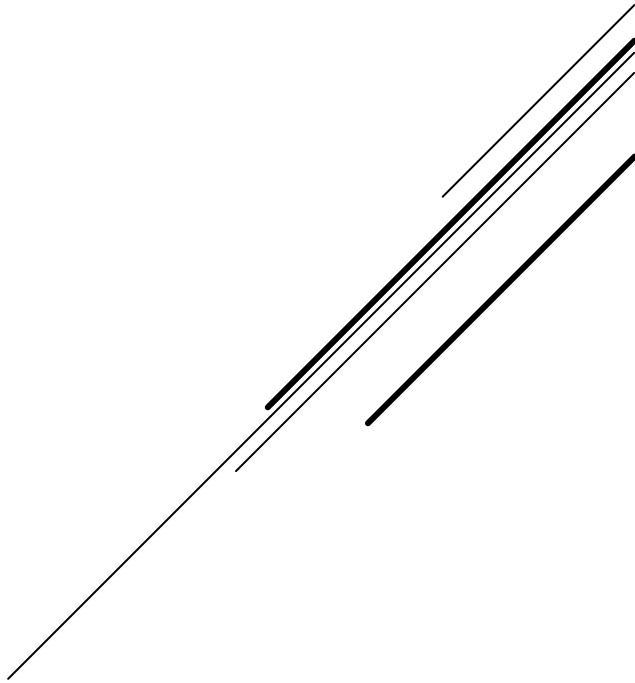






B. KLUCZE, ADRESY, TRANSAKCJE

NA PRZYKŁADZIE BTC



BITCOIN [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

- 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 odnoście 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 $

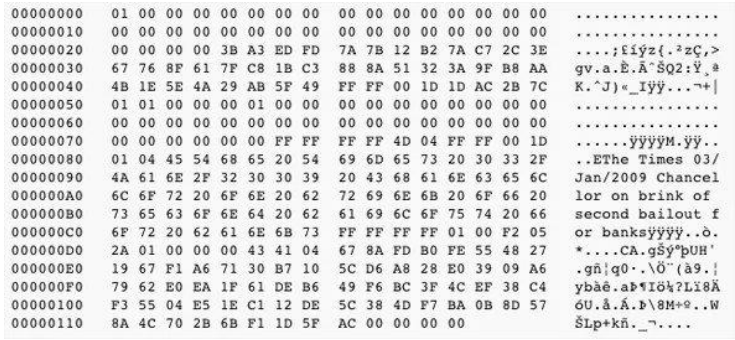
…

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)
  - …
- $210000 \cdot (50 + 25 + 12.5 + \ldots) \rightarrow 21000000$
- blok jest wydobywany średnio co 10 minut
- nowe BTC generowane są *ex nihilo* (z niczego)

SKĄD LICZBA 21 000 000 BTC?

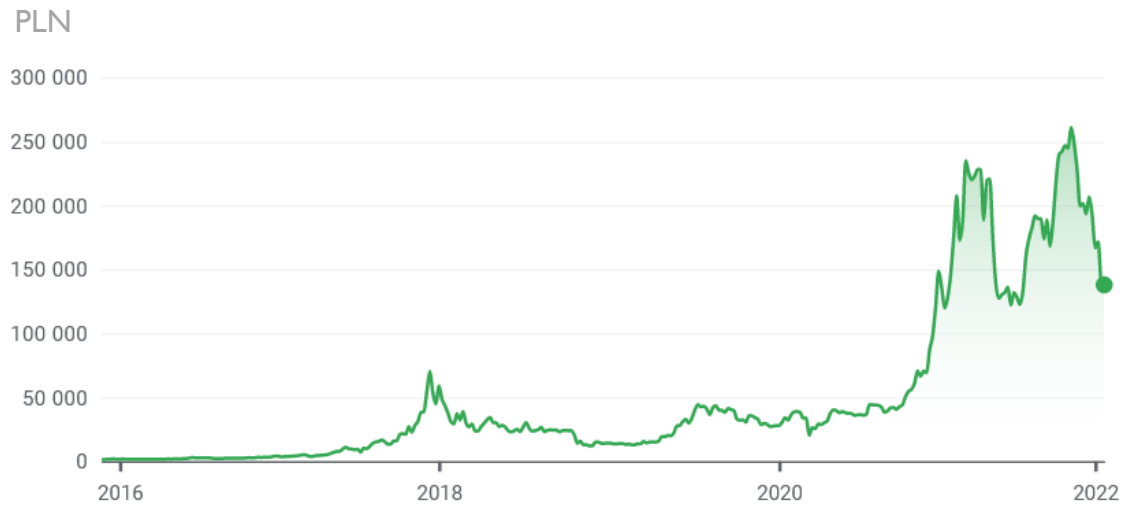
- Pierwsza transakcja
  - 3 stycznia 2009 roku o 20:15:05 UTC
    Satoshi Nakamoto wygenerował pierwszy blok
- Pierwszy transfer
  - 12 stycznia 2009 roku Satshi Nakamoto przesyła 100BTC do Hala Finnera z PGP Corporation
- Najdroższa pizza (pierwsza płatność)
  - 22 maja 2010 roku Laszlo Hanyecz, informatyk 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



POWOLNY POCZĄTKOWY ROZRUCH PROJEKTU

PIERWSZE KURSY BTC

- 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)



How a ₿itcoin 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.

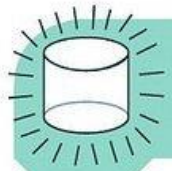
WALLETS AND ADDRESSES

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 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

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.

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.

Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

SUBMITTING A PAYMENT

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

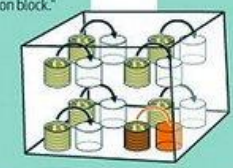
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

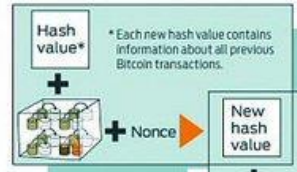
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

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



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



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

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 veil	b8db 7ee9 8392...

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.

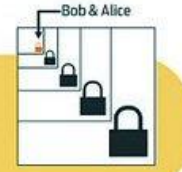
The root of all evil ???	0000 0000 0000 ...

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.

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.

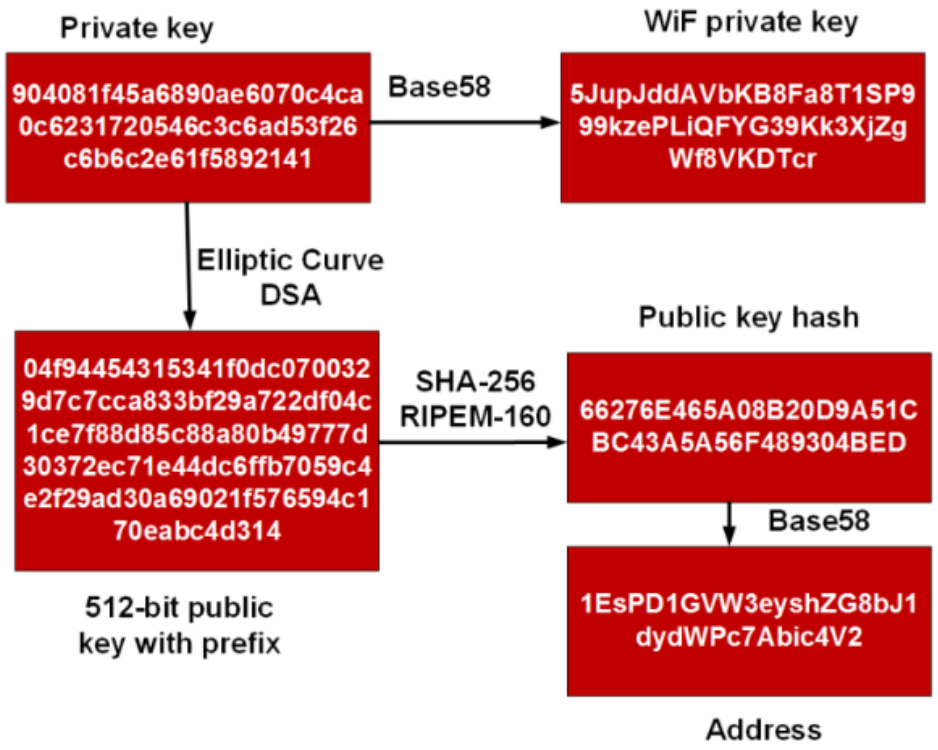
TRANSACTION VERIFIED

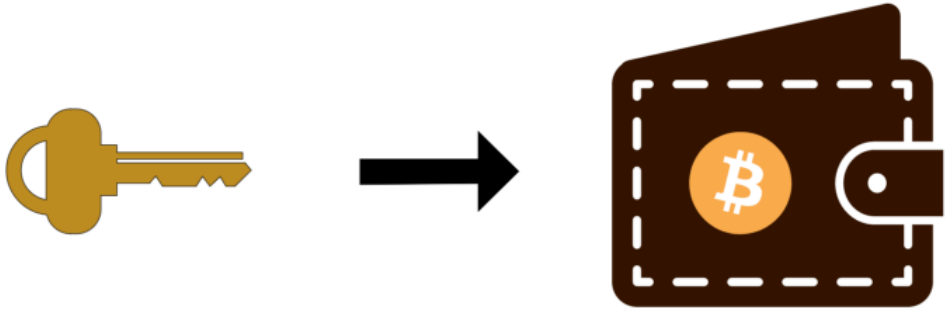


As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat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

TWORZYMY ADRES BTC

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





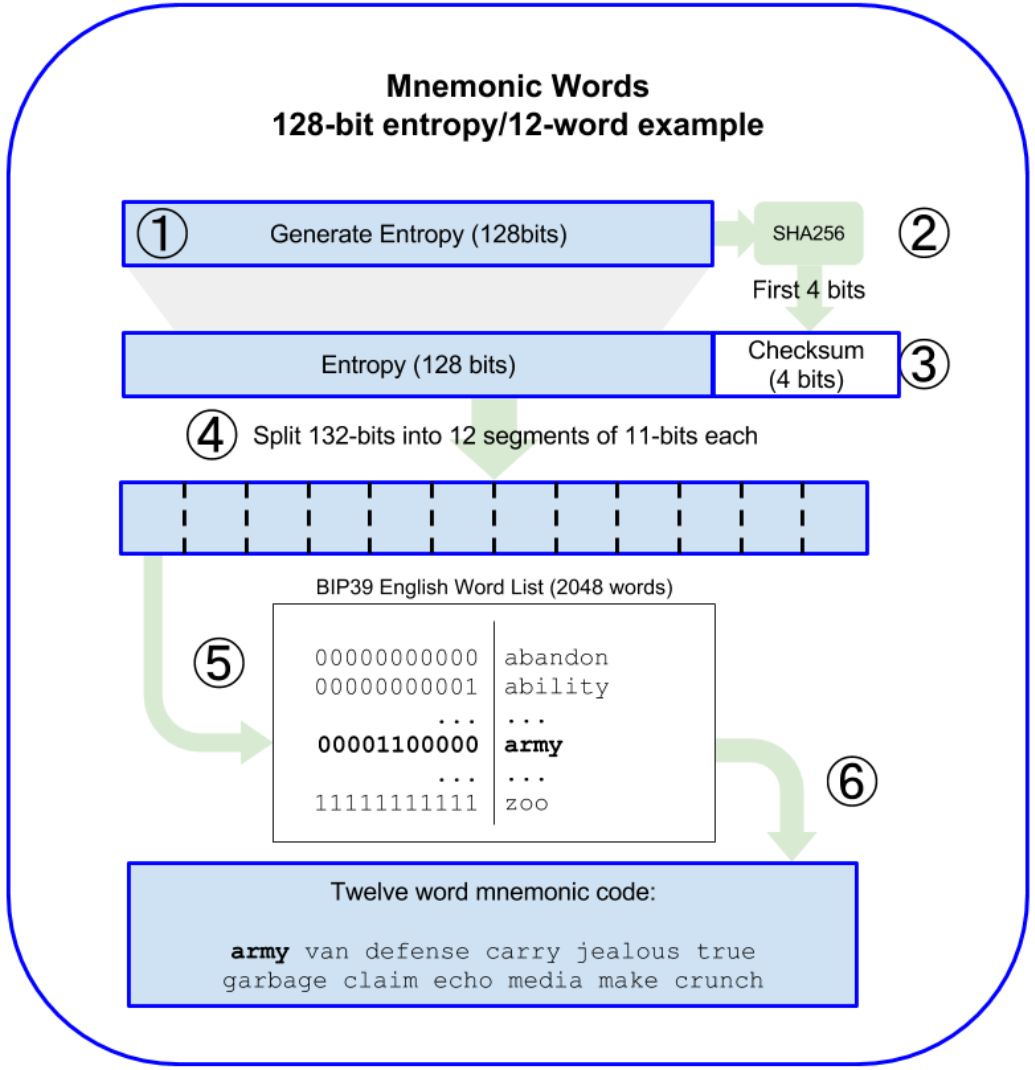
klucz prywatny – pełen dostęp do środków

OD KLUCZA DO ADRESU

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

A CO MA DO TEGO SEED?

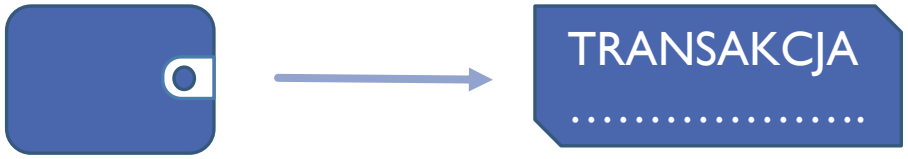
- Kod mnemoniczny (ang. seed *) to inna „forma zapamiętania” liczby losowej
  - liczba ta będzie wykorzystana do utworzenia klucz prywatnego **k**
- Kod mnemoniczny stanowi ciąg 12 - 24 wyrazów w danym języku
  - English 日本語 Español Français Italiano …
- Standard BIP-39 zaproponowany przez producenta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

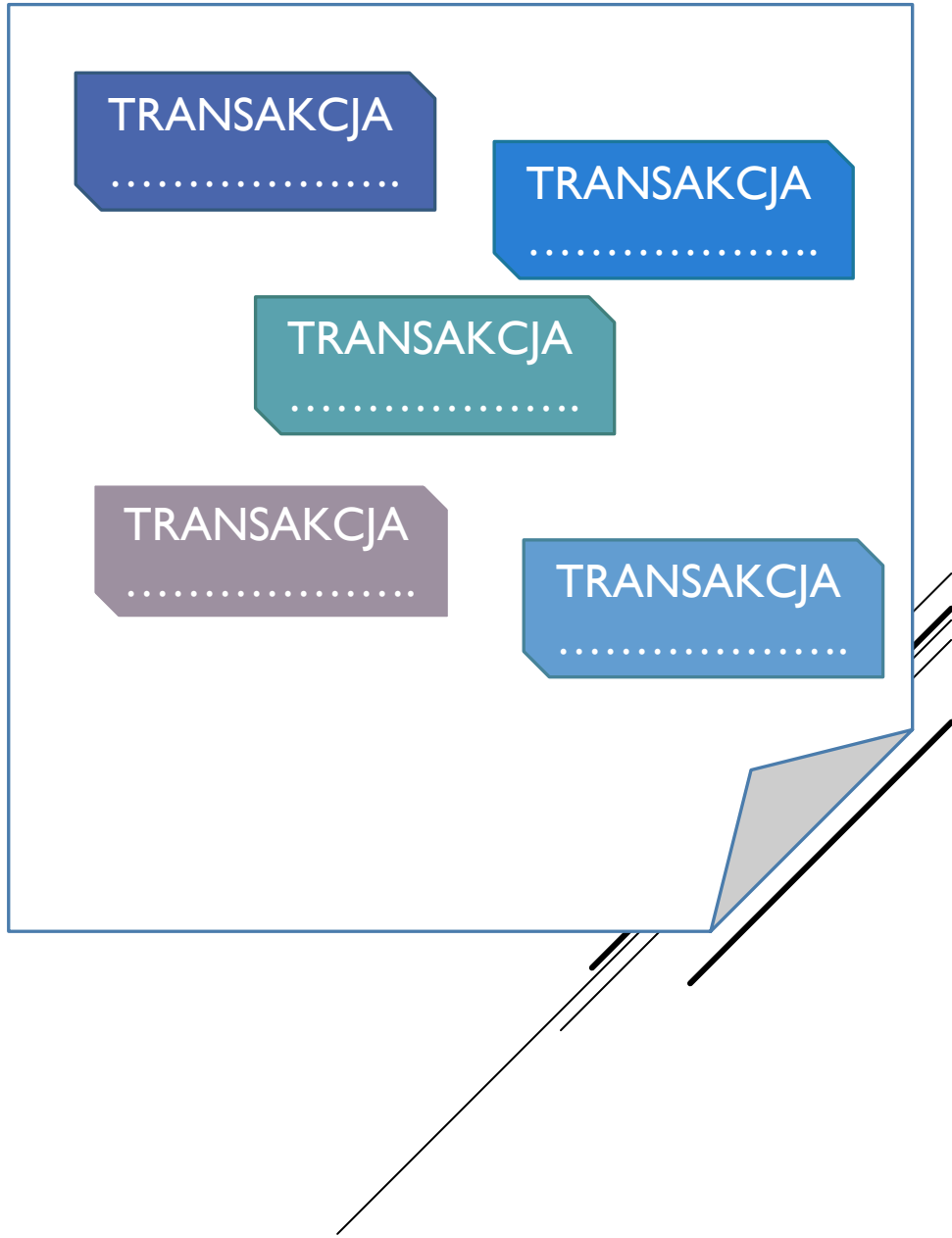


JAK JEST WYBIERANY KOD MNEMONICZNY

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

wizualizacja nowych transakcji http://bitcoinrain.io/

Z MEMPOOL-A DO BLOCKCHAIN-A

- „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 hashem 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. 6.25 BTC)

C. PSEUDOANONIMOWOŚĆ

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

Transakcja Zobacz informacje o transakcji bitcoin

63c5f2ec7d5a88265e26f687a532dfe5b5071c9971beb2decddab135cb4696d2

13X8swZWP54N6C9La1M9QfzPcSWWUNUnbg	1JYQKbrMgeHHydNzMCaJe2VtpwmSjMW7wf	0.0198 BTC
	15zdGLs5u7Z5z2j16qJVpjwsRn1wMPJBnG	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)
Potwierdzeń	1 Potwierdzeń
Wizualizacja	Zobacz wykres drzewa

Przychody i wyjścia	
Razem przychodów	0.02736749 BTC
Razem wychodzących	0.02636749 BTC
Opłaty	0.001 BTC
Opłata za bajt	444.444 sat/B
Opłata za jednostkę wagi	111.111 sat/WU
Szacunkowa ilość BTC w transakcji	0.00656749 BTC
Skrypty	Pokaż skrypty & coinbase

BLOK I TRANSAKCJA

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

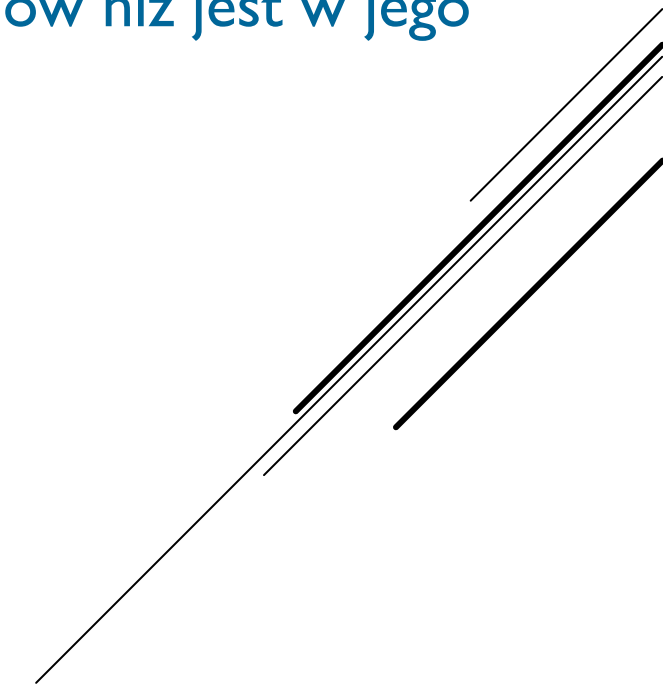
Brak wejść (nowe monety wygenerowane)		1C1m
		Nie mo

63c5f2ec7d5a88265e26f687a532dfe5b5071c9971beb2decddab135cb4696d2

13X8swZWP54N6C9La1M9QfzPcSWWUNUnbg		1JYQ
		15zd

TRANSAKCJE – ZASADY 1

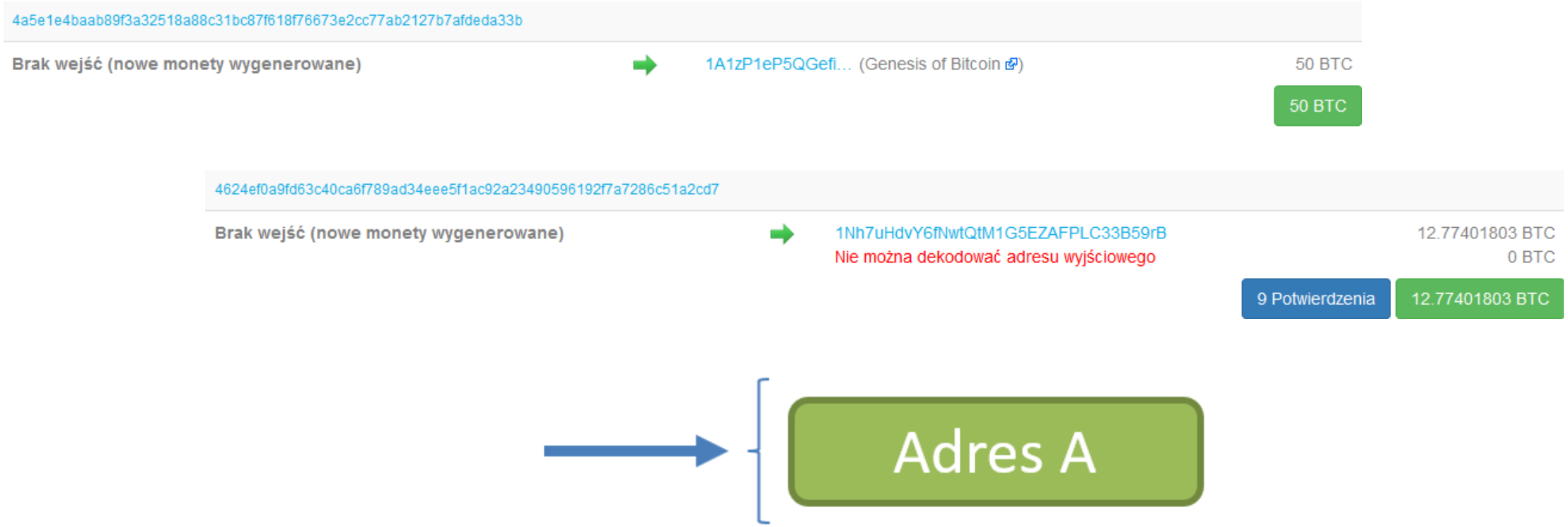
- Tylko niezerowa liczba bitcoinów może być przesyłana z jednego adresu na drugi.
- Każda transakcja składa się z dwóch stron: wejściowej i wyjściowej.
- Adresy znajdujące się po stronie wejściowej, zwane dalej w pracy adresami wejściowymi, muszą posiadać wystarczającą liczbę bitcoinów dla danej transakcji. Nie ma możliwości przesłania z danego adresu większej liczby bitcoinów niż jest w jego posiadaniu.



TRANSAKCJE – ZASADY 2

- 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.

- Większość transakcji znajdująca się w łańcuchu bloków zawierają opłatę transakcyjną.
- Liczba bitcoinów znajdujących się po stronie wejściowej transakcji musi być równa liczbie bitcoinów znajdujących się po stronie wyjściowej transakcji powiększonej o ewentualną opłatę transakcyjną.



RODZAJE TRANSAKCJI 0 → 1

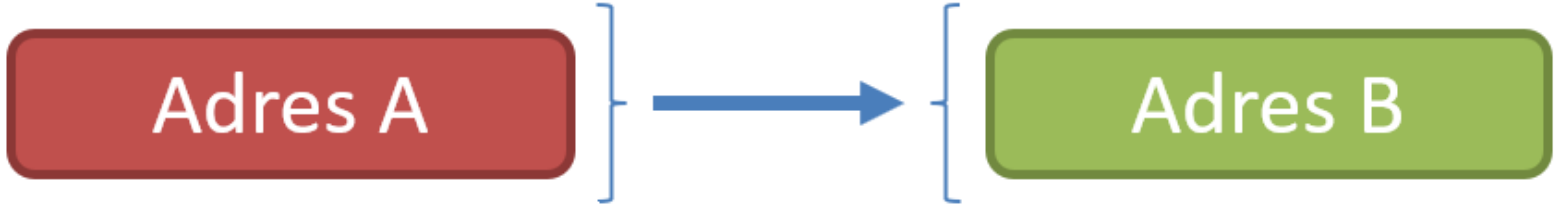
281b0e73b30f2bbb4f1859ed432cceb9e1431418794b27247f72ea834da73268

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
Opłaty	0.00000691 BTC



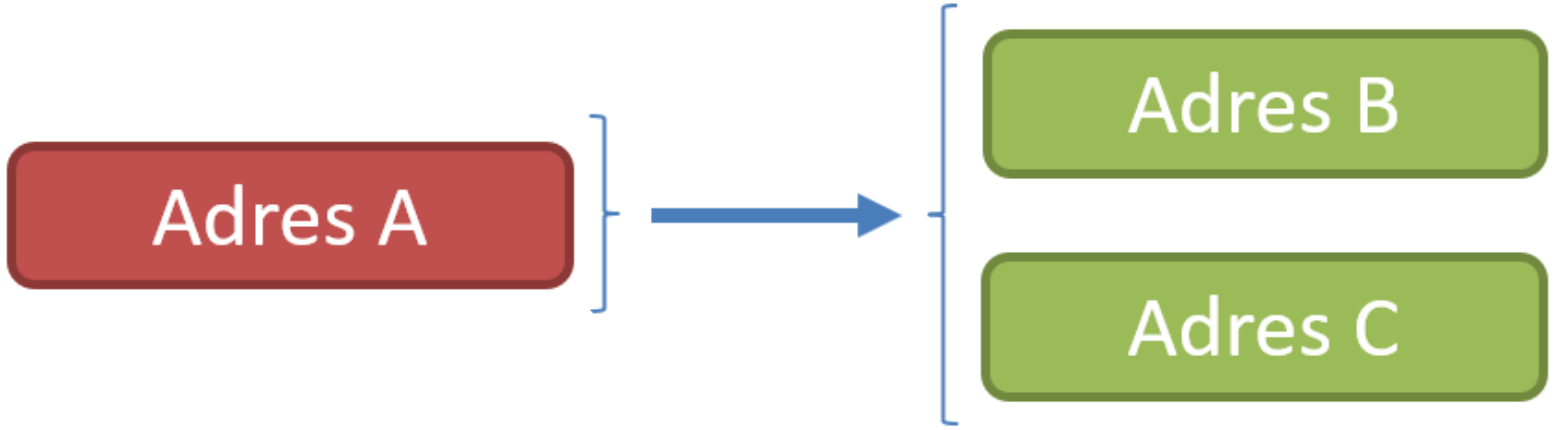
RODZAJE TRANSAKCJI 1 → 1

3c6409ecb159df64d59a55b9368a40787b4dd7eed721a11593c1b04e6e5328a5

1CuBgumLwcR2gSac6nW23uWuhMqVs6TwUg	→	1KLpmhwuiF4JhPJ8e7p6nFFbeChCzirSq8	89.38738 BTC
		1KYMJ5T5YJkLN7LYgs9Rrzj7FCvqWPjq6j	0.18 BTC
			89.56738 BTC

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

Przychody i wyjścia	
Razem przychodów	89.5676286 BTC
Razem wychodzących	89.56738 BTC
Opłaty	0.0002486 BTC



czasami Adres A = Adres C

RODZAJE TRANSAKCJI 1 → 2

57,93%

3b978e586018d51de04e1a2624081bf0f9679b40af5aada49a903607fc3a052b

1KYMJ5T5YJkLN7LYgs9Rrzj7FCvqWPjq6j 1MUqFqUZsB6BKppMPRkah5cnQYp77ZAwzn 1LfkzuF6Hr86wRWCtWBsa2vefqWKKZmQJ5 1HgEKpzKzQ98EfGALcUF32Ngn4aAcivG1A 1LhCu8jh8AVLEm9qETAQBX3PHqJNhDnmvQ 1MRsGAVUJnm1PkxhuwVkZqmpKG2ec6EFLa 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 wyjścia	
Razem przychodów	4.6317288 BTC
Razem wychodzących	4.63 BTC
Opłaty	0.0017288 BTC

RODZAJE TRANSAKCJI N → 1

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

Przychody i wyjścia	
Razem przychodów	1.41353384 BTC
Razem wychodzących	1.41111784 BTC
Opłaty	0.002416 BTC

RODZAJE TRANSAKCJI N → 2

21,74%

4dab9ccd4c42043080ffaf1711fe4430dad854b966c79d890059ca9d1f9e7091

19NaxUoUWEJLZXzwnahi9wjf16HoUjWB6o	1pKNa39SaGzjv2B3PhWTA62Pku1XUHv9d	1.683572 BTC
1BZoJ5A8DZY2wk2dkrFCYcNp3m4wHpoggM	1EWkz13EfEHFcEmu52MMiMJhcV5GfECTCE	8.364422 BTC
13phPJ4a8yjo7uYqBEqNpPCw3YF4yYRvjr	19f2WKJ2ibfG1Rzp9RNaURDiciL6PKq7xF	1.091 BTC
1CPMLny76P1Myk9B78hJBHa1t8YSWFYsGM	1MaKPepS4vPxn5n4TGpkcTwosMG5oPcwhZ	1.10550838 BTC
112ch8mPU9r4R7gtTvPUU7UgR1GR2bEUoh	12NW2eWA95a6bjuDmpbJj4LhbcwpyDScav	7.021222 BTC
12u3DDXzR4Q9m5uUrPYxpucJ4eoYq5rdDi	15BEVbxtYT8AQTZe6gbWyxeQDoEHZnyghZ	1.11068017 BTC
1pgJ4AoUrgroiqFgL8zoSiX8kuZQ4Vhsq	1JGNAwQRqmngzu2pfr2t3K3pY82s5CbTwq	1.019 BTC
1C66sXCXGa7uA2PYkiTfAZf5aG8C5CyejP	15cXikA1U6gWnoXsQGKVh98sTvQbYRcuAZ	1.144 BTC
1JYqeUrjcP3R2PiWq2cazDfjNK6JifF9zG	1MvYxmpag6xwrPKZoraKAJjvcahfnhx44	1.0884 BTC
19emG7L4Cu53229H7S44SpevtHtGhWyseT	1CoN7sh1gyCqkH9KJzVX6oFQm7wa6L6kXB	0.993 BTC
1DYjKcvEWbuSsMKVuopYvpembYcnVcstoB	1JbwR7Nu9B1rTcdppqkgum9JVSmLiakuWc	1.1471 BTC
1HmZ9HQX38edAbpkT98TdG2jVmkzEtMmpE	1JYqeUrjcP3R2PiWq2cazDfjNK6JifF9zG	0.15417011 BTC
1K8K6Agh5TX3y6wrf1g1i3WL8UAbebuEEP	1Eyj7mh4wicN3TddTvyoHH5C2CkWsRM4uc	1.07665831 BTC
1Mp5RFhhWCwjKapnQfgJreSgJ4CChHx4Xa	1KdvDgrK9rjNsWnTmSFkC5oXgAn58rGvmn	1.04840443 BTC
1GbFwTPqcdfzDku5431UWze4RKjC77NVJ7	12uK2YyVG4urGmarZEfLVYSnsFXr1Ujtgf	1.11200831 BTC
1KjJtuN4znGkd77bwcBTuWzHCZpY5WPzYx	19xUAF4u5SafZrncHMC9FBFKzMyXSehaxp	1.119581 BTC
15wsVKy11BScmrBhgNFYWwDmir7XdALfkc	1BKirpHM9xwMLrgjiUTox5BSzKujxUanFF	1.040242 BTC
1KBPLnSaLhLgSxjmDwEspjiL7ZHjFDajNH	15DMH9GpNFxbSdLxdMHngcY2xf3qYn6dch	1.0477404 BTC
1Nm7995VV54mzUp7K7VN2enNP5yVAF4BWq	1C34GFcC4Xe1rU7Q6298zP8FL3WBD3MQgU	0.9835 BTC
13SGQp1MR1otMRJi4yGMRRpQRz1mtpxUQA	13eRtad7LBwHbTJZ11XMa7sit3ZHwpRT1U	1.083597 BTC
1GYYTHDjyG8C7Dx4r9PuxEMTyTmxCd317X	1PXrwjGa5XNrFzZYhyJWkXU54AAtvjZ99a	1.13 BTC

35.56380611 BTC

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

Przychody i wyjścia	
Razem przychodów	35.56430611 BTC
Razem wychodzących	35.56380611 BTC
Opłaty	0.0005 BTC

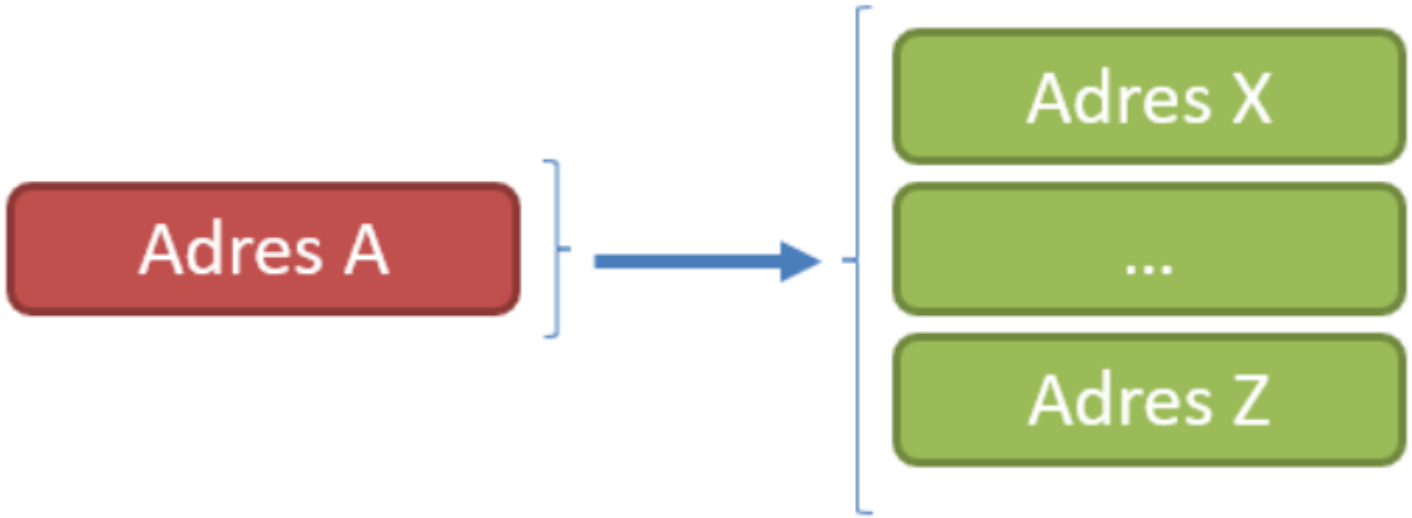
7957151ab2ac8ad51a6117c0e56baf4e8a769f93a603b9ea8e2b2f66c5b37536

1GXerksFNbckEmQBt7fT4Vu97hRZNQVzna	1EHRiH14C7ojKAX7H3AWxmXHQxGrizQJwa	0.01 BTC
	1KuuHVAbJSnfkYf93wmUf1WJUQhFx2Dntn	0.74794977 BTC
	1Bs4F9sBNeTnV6EE9jjq3DoYn6Vq1LR4Yz	0.01 BTC
	1BBnMCFjf5KijJwRGzZdVdvrx8mxMKx9Y2	0.01 BTC

0.77794977 BTC

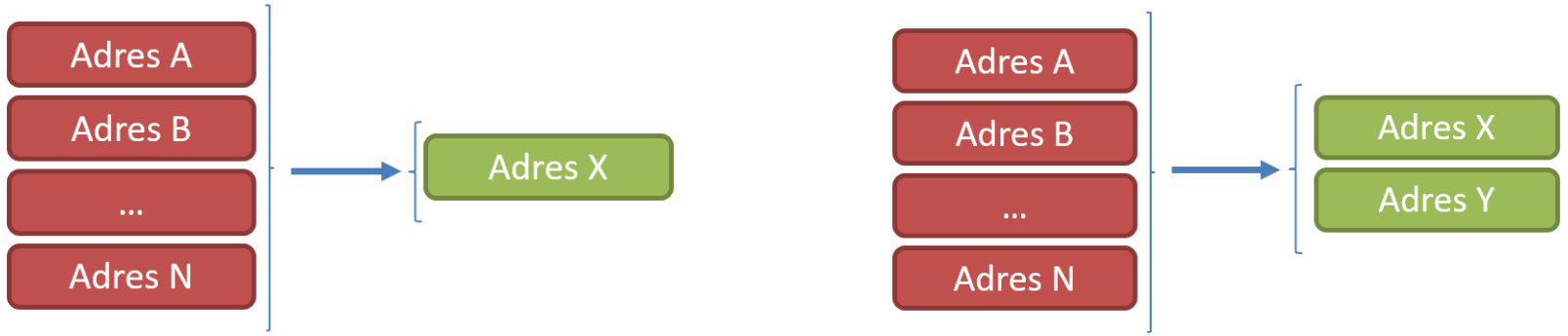
Podsumowanie	
Rozmiar	294 (Bajtów)
Waga	1176
Czas otrzymania	2016-07-09 23:26:37

Przychody i wyjścia	
Razem przychodów	0.77839253 BTC
Razem wychodzących	0.77794977 BTC
Opłaty	0.00044276 BTC



RODZAJE TRANSAKCJI 1 → 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.

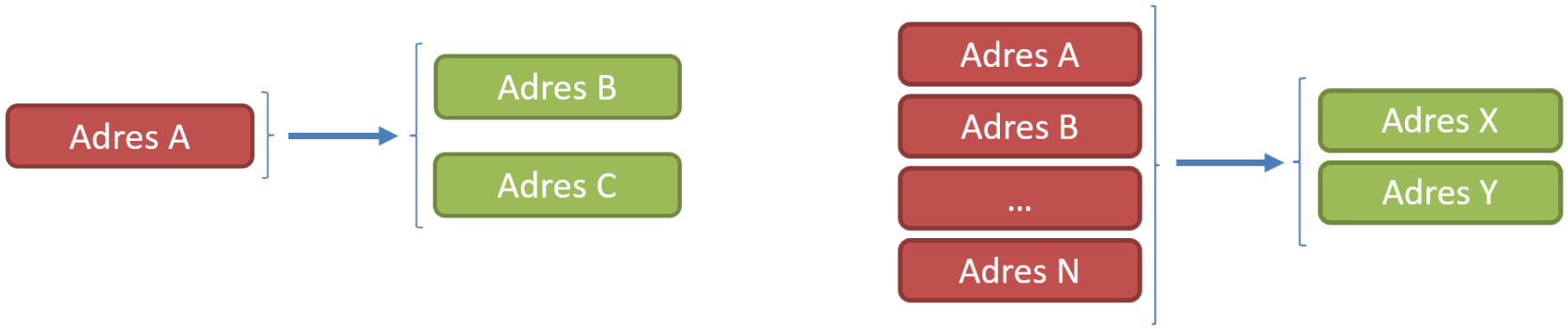


HEURYSTYKA 1

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

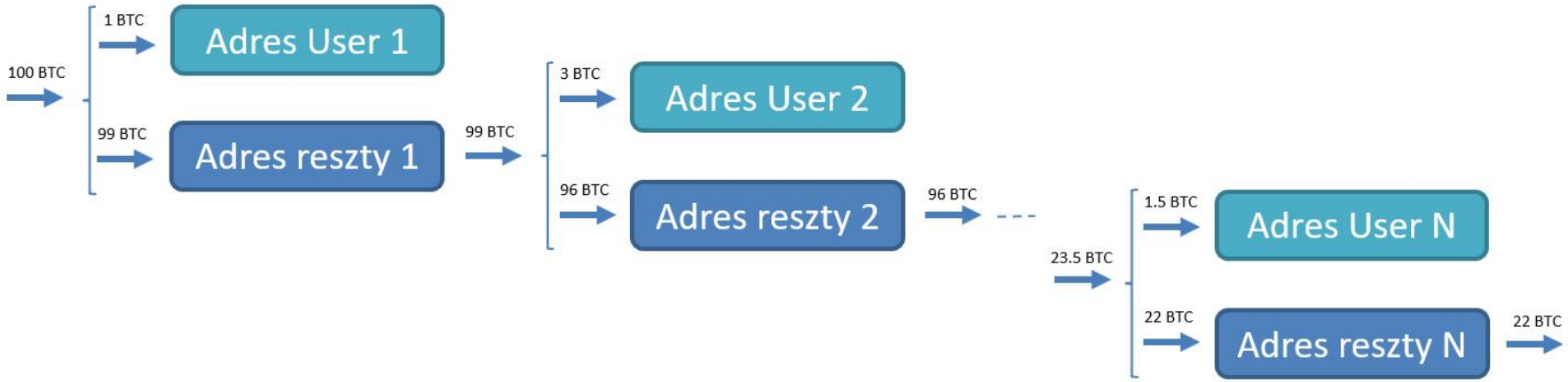
HEURYSTYKA 2

- 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?

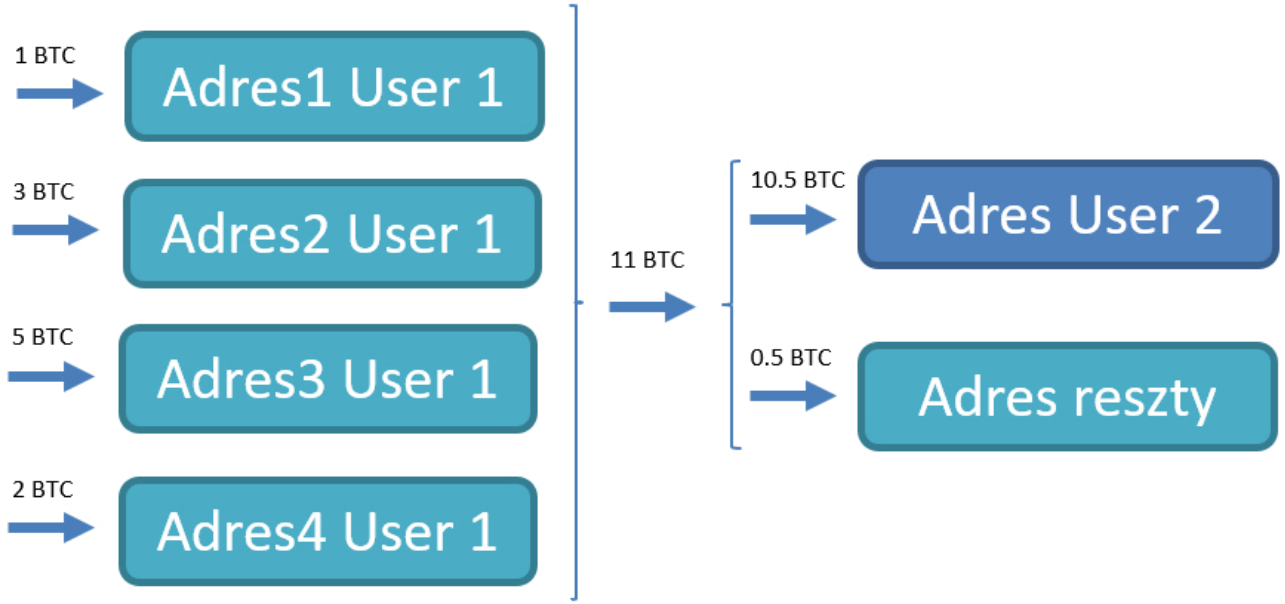


- sprawdzenie czy jeden z adresów nigdy wcześniej nie występował z łańcuchu bloków
  - jeśli tak, to można z dużym prawdopodobieństwem założyć, iż jest to właśnie adres reszty, gdyż wiele portfeli bitcoinowych działa właśnie w ten sposób – tworzy nowy adres dla kwoty stanowiącej resztę transakcji

HEURYSTYKA 2
ADRES RESZTY – SCENARIUSZ 1



HEURYSTYKA 2
ADRES RESZTY – SCENARIUSZ 2



HEURYSTYKA 2
ADRES RESZTY – SCENARIUSZ 3

ETHEREUM [ETH]

- 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, crowfunding

METODY OSIĄGANIA KONSENSUSU

- 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, …
- …

INNE KRYPTOWALUTY

- Anonimowość: Monero, Zcash, …
- Pożyteczne: Primecoin, …
- Stablecoiny: Tether, …

- Blisko **10 tysięcy** projektów
  - https://www.coinlore.com/all_coins

Bitcoin	BTC	Digital gold
Ethereum	ETH	Programmable contracts and money
Bitcoin Cash	BCH	Bitcoin clone
Ripple	XRP	Enterprise payment settlement network
Litecoin	LTC	Faster Bitcoin
Dash	DASH	Privacy-focused Bitcoin clone
NEO	NEO	Chinese-market Ethereum
Monero	XMR	Private digital cash
Ethereum Classic	ETC	Ethereum clone
IOTA	MIOTA	Internet-of-things payments
Zcash	ZEC	Private digital cash
Tether	USDT	Price = 1 USD

…

Źródło: https://techcrunch.com/2017/11/19/100-cryptocurrencies-described-in-4-words-or-less/

A. Zasada działania kryptowalut, łańcuch bloków

B. Klucze, adresy, transakcje

C. Pseudoanonimowość

PYTANIA?