Gawęda o kryptowalucie Bitcoin

informatykzakladowy.pl

Gawędę sponsoruje słowo „uproszczenie”

Nie kupuj bitcoinów mając tylko wiedzę z tej prelekcji. Ucz się i ćwicz na małych kwotach!

- Funkcja skrótu (funkcja haszująca)
- **Blockchain**
- Sieci P2P
- **Rozproszony rejestr**
- Kryptografia klucza publicznego
- **Generowanie jednostek kryptowaluty**
- Regulacja trudności tworzenia bloków
- **Konsensus i proof of work**
- Co to jest kopalnia i czym się kopie bitcoiny
- Do czego komu Bitcoin i kto to w ogóle wymyślił
- Zastosowania blockchaina (buhahahahahahaha)

Funkcja skrótu

(funkcja haszująca)

slido.com
#76766

Funkcja skrótu (funkcja haszująca)

- Funkcja w rozumieniu matematycznym – przyjmuje argument (ciąg bajtów dowolnej długości), dokonuje przekształcenia jednokierunkowego i zwraca wynik zwany haszem albo skrótem (też ciąg bajtów, ale stałej wielkości)
- Gdy patrzymy na skrót (na przykład taki jak poniżej), nie potrafimy powiedzieć niczego o wejściowym ciągu bajtów, jedyna możliwość znalezienia go to przejrzenie wszystkich możliwych takich ciągów

  b7d2998ad349eb1af339a94fb3b4e3dfdd169c181b72afd0839924cf25e34150

- Nie potrafimy generować kolizji (dowolnych ani dopasowanych)

Funkcja skrótu - przykład

Wejście (dowolnie długie):
Litwo, ojczyzno moja

SHA256 (zawsze 32 bajty):
5d825022bd617f7ab3b773ef37f75ec475a1905308db0fb91050ed24065ba2e1

Wejście (dowolnie długie):
cały tekst Pana Tadeusza w formacie txt z wolnelektury.pl

SHA256 (zawsze 32 bajty):
b7d2998ad349eb1af339a94fb3b4e3dfdd169c181b72afd0839924cf25e34150

Funkcja skrótu (funkcja haszująca)

- Funkcja skrótu ma zachować się jak funkcja pseudolosowa, tzn. jeśli weźmiemy dwa dowolne ciągi wejściowe i obliczymy ich skróty, to średnio 50% bitów będzie się różnić
- Zmiana jednego bitu wejścia zmienia średnio połowę bitów skrótu

- Przykładowe zastosowania
  - Zapis skrótów haseł zamiast haseł
  - Dowód istnienia dokumentu w określonym czasie

- Złe funkcje: MD5, SHA-1; dobra funkcja: SHA-2

Blockchain

łańcuch bloków

slido.com
#76766

DEMO

Blockchain (block chain)

- Rejestr, do którego można coś dopisać ale nie można (w sposób niezauważony) zmienić niepostrzeżenie ani jednego wcześniejszego zapisu
- Aby samodzielnie zweryfikować integralność blockchaina, trzeba mieć dostęp do kompletu danych

- Bitcoin na początku 2021: 660 tys. bloków, 311 GB danych

Sieci P2P

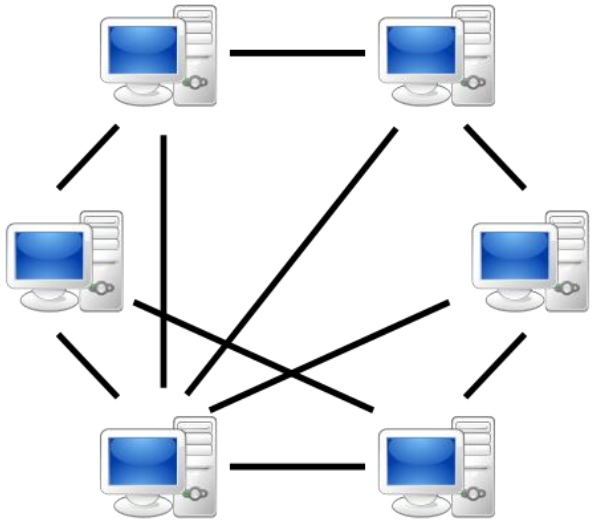
peer-to-peer

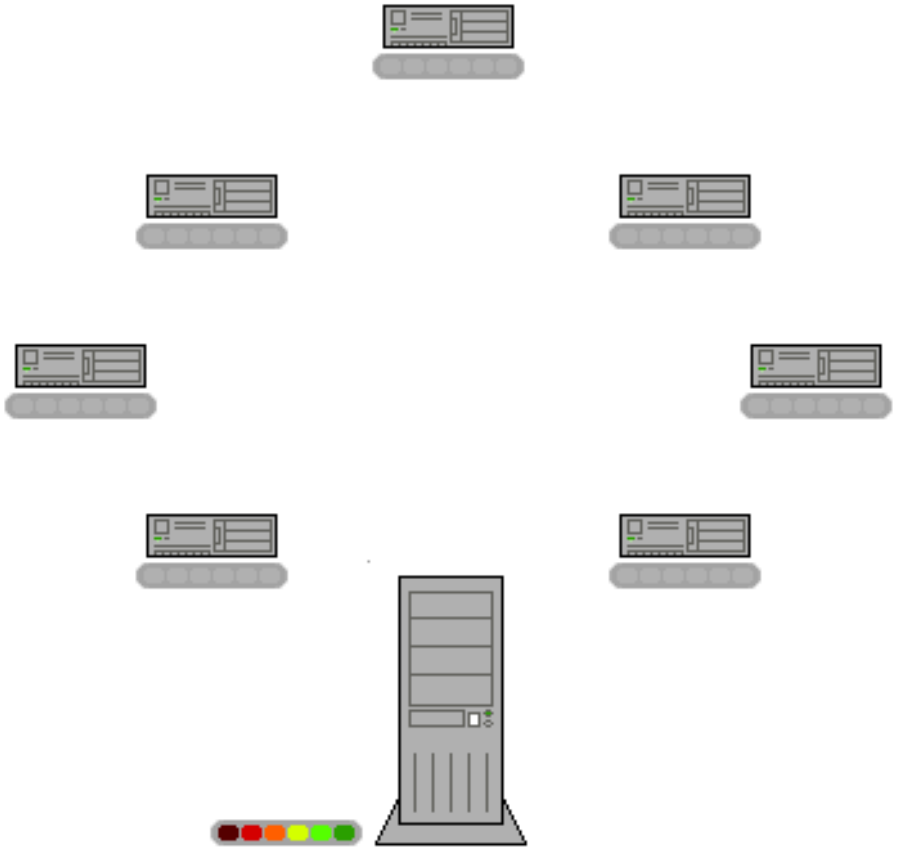
slido.com
#76766

P2P (peer-to-peer)

- Model komunikacji w sieci komputerowej zapewniający wszystkim hostom te same uprawnienia

- Bittorrent!





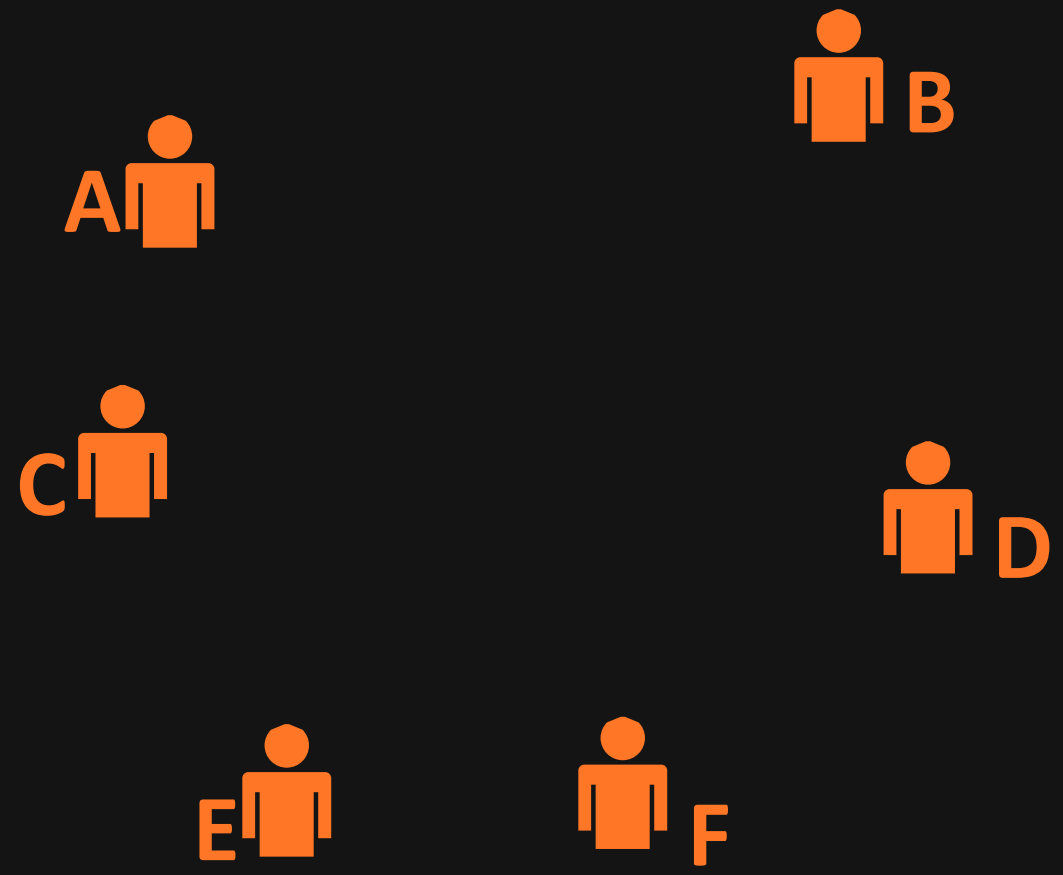
Rozproszony rejestr

Rejestr scentralizowany

Banki zapisują wpłaty i wypłaty

- A wpłacił 10 tys. na lokatę
- D zaciągnął 15 tys. kredytu
- Bank obciąża konto D kosztami 1000 zł odsetek
- Bank uznaje konto A kwotą 100 zł
- C wpłata 5 tys. na lokatę
- itd.

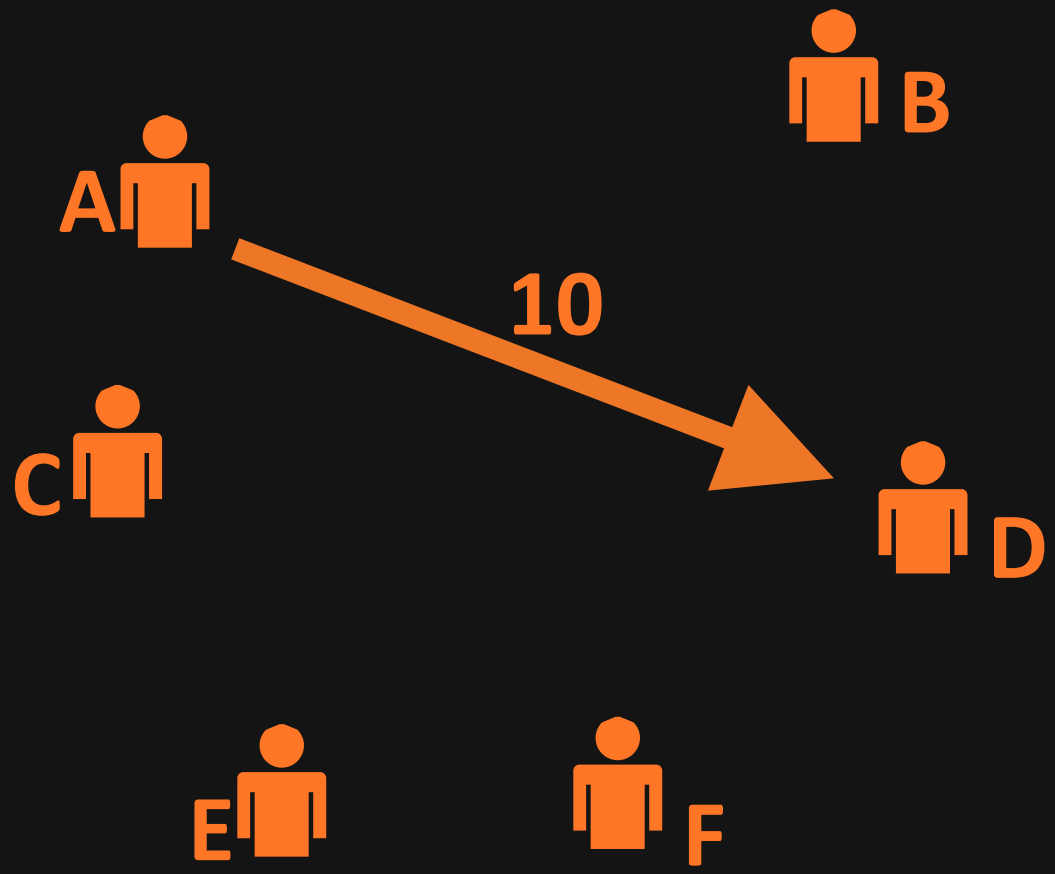
Rejestr pożyczek



Grupa znajomych

A → D, 10

Rejestr pożyczek

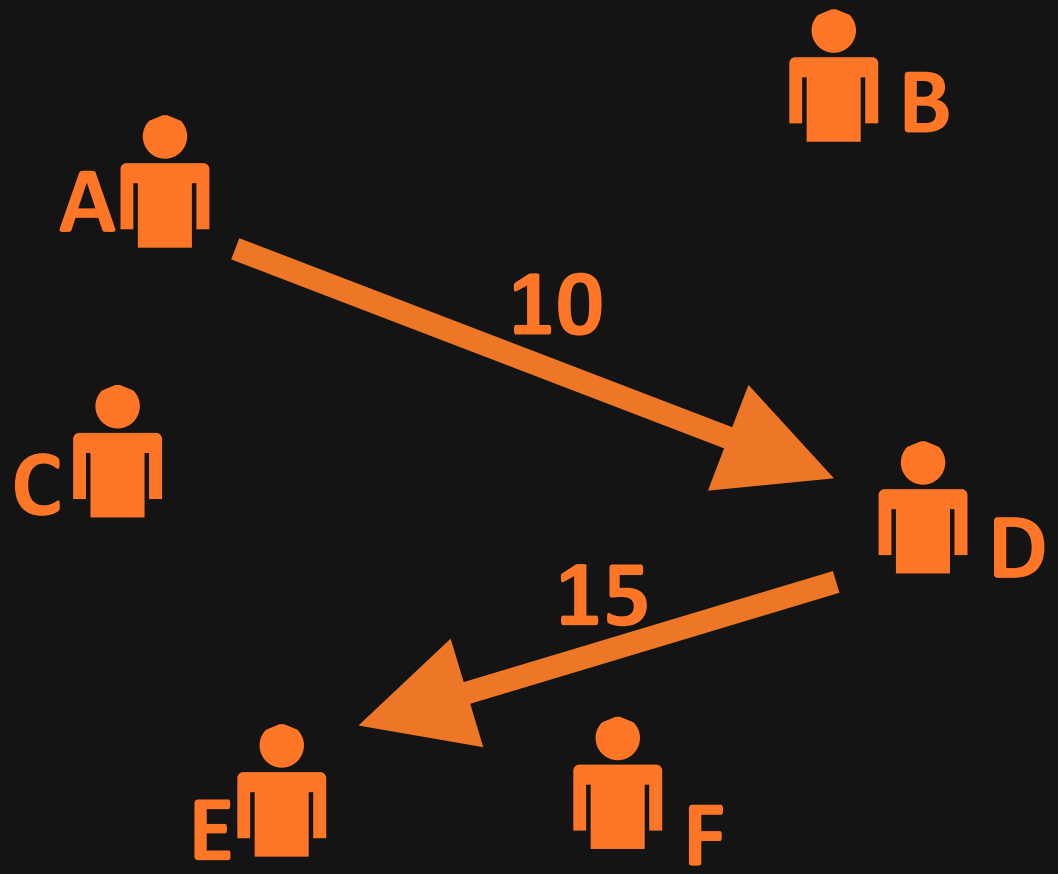


Grupa znajomych

A → D, 10

D → E, 15

Rejestr pożyczek



Grupa znajomych

A → D, 10

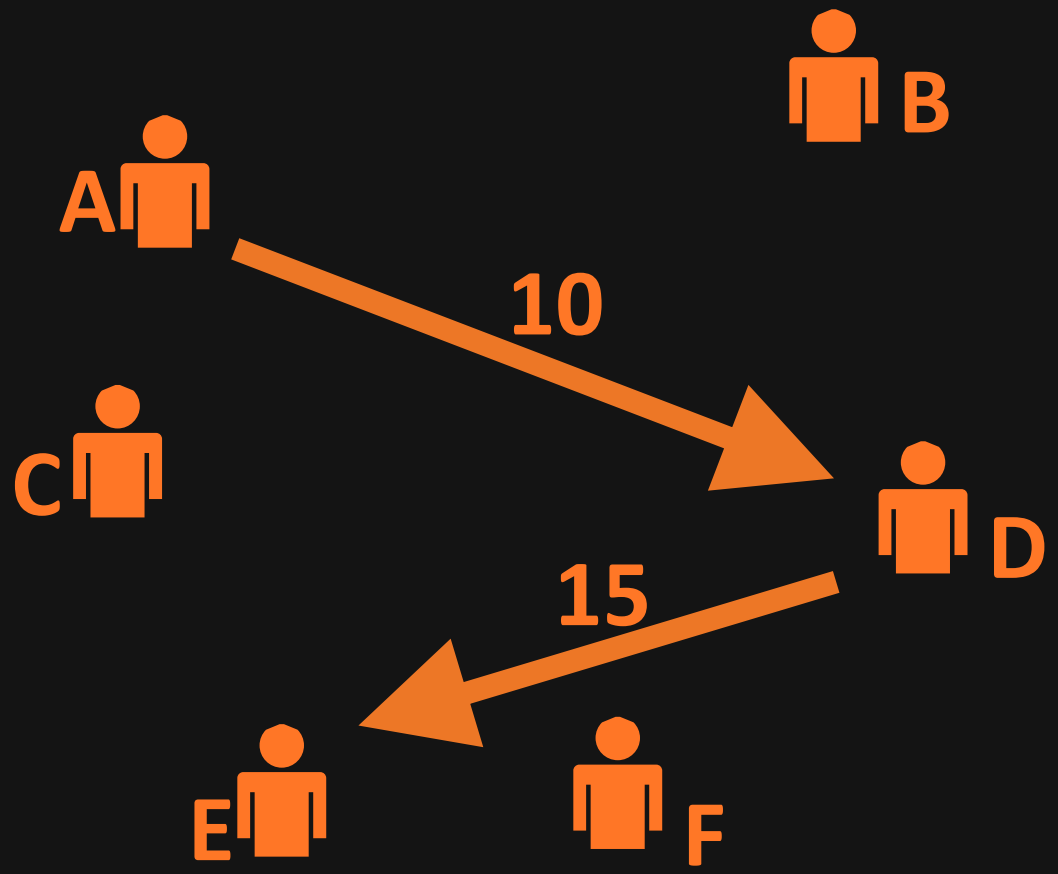
D → E, 15

… → …, …

… → …, …

… → …, …

Rejestr pożyczek



Grupa znajomych

A → D, 10

D → E, 15

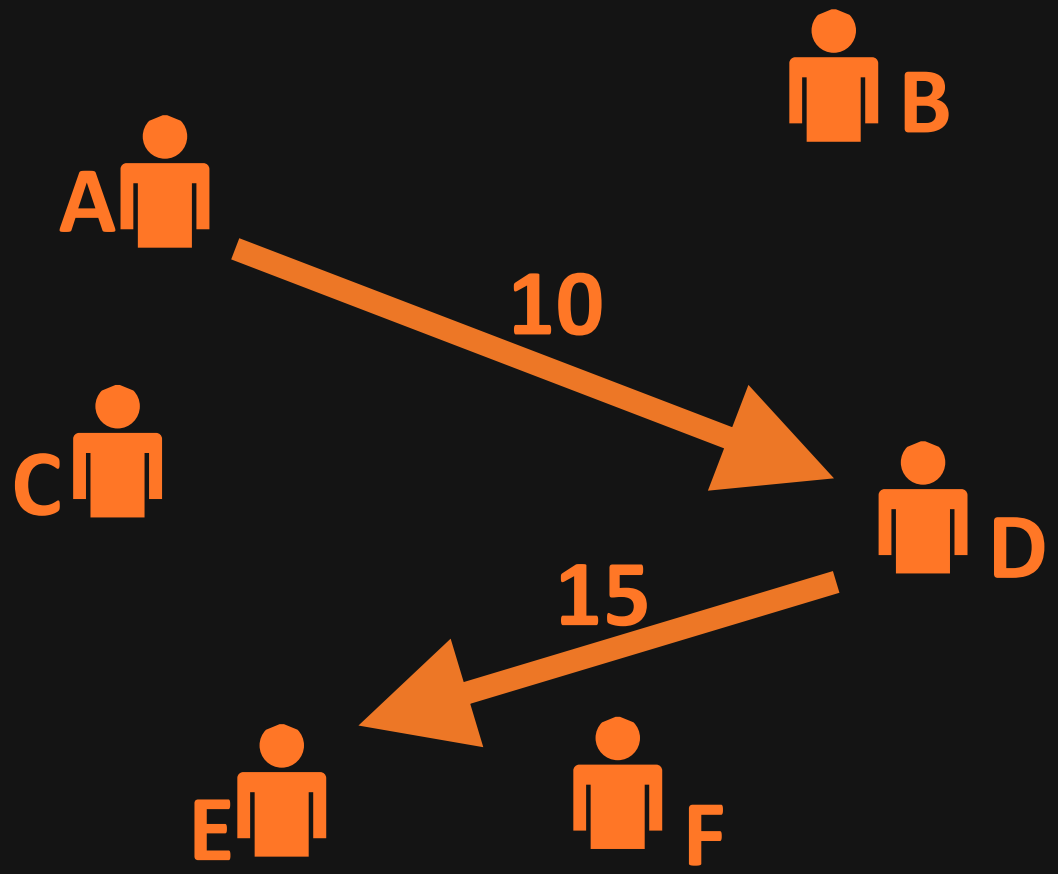
… → …, …

… → …, …

… → …, …

5d825022bd617f7a

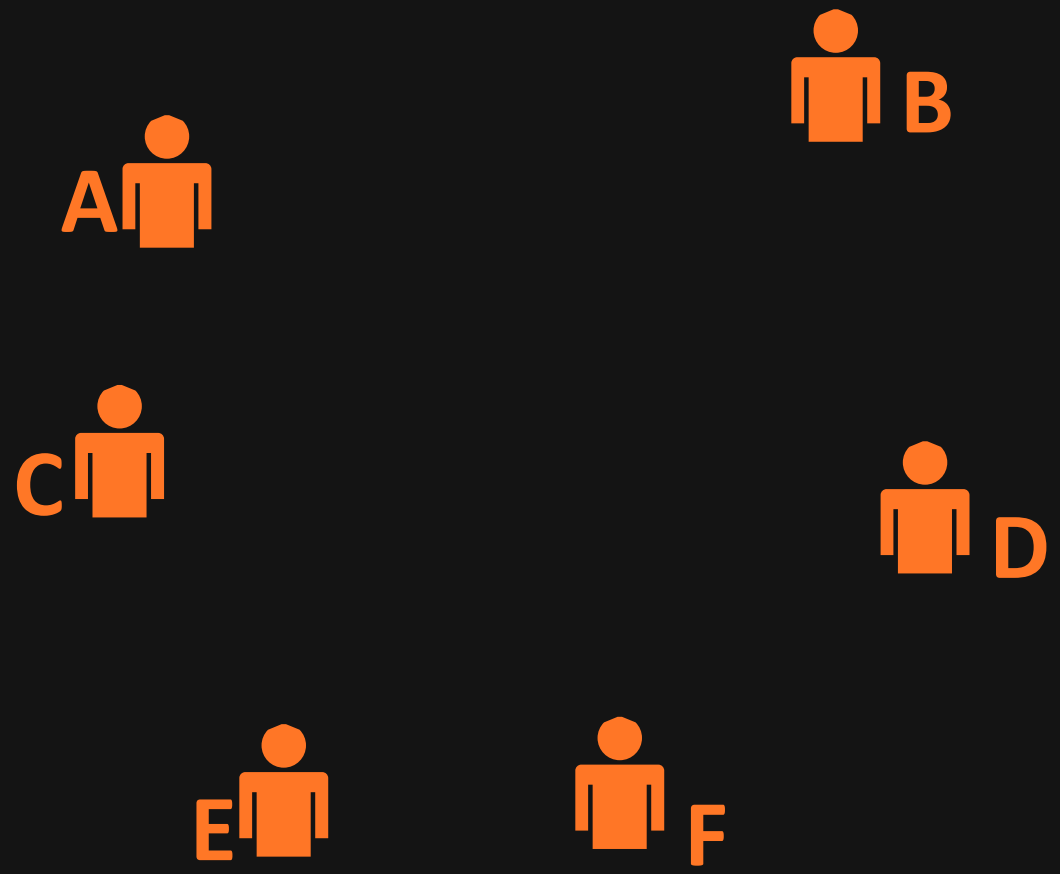
Rejestr pożyczek



Grupa znajomych

5d825022bd617f7a

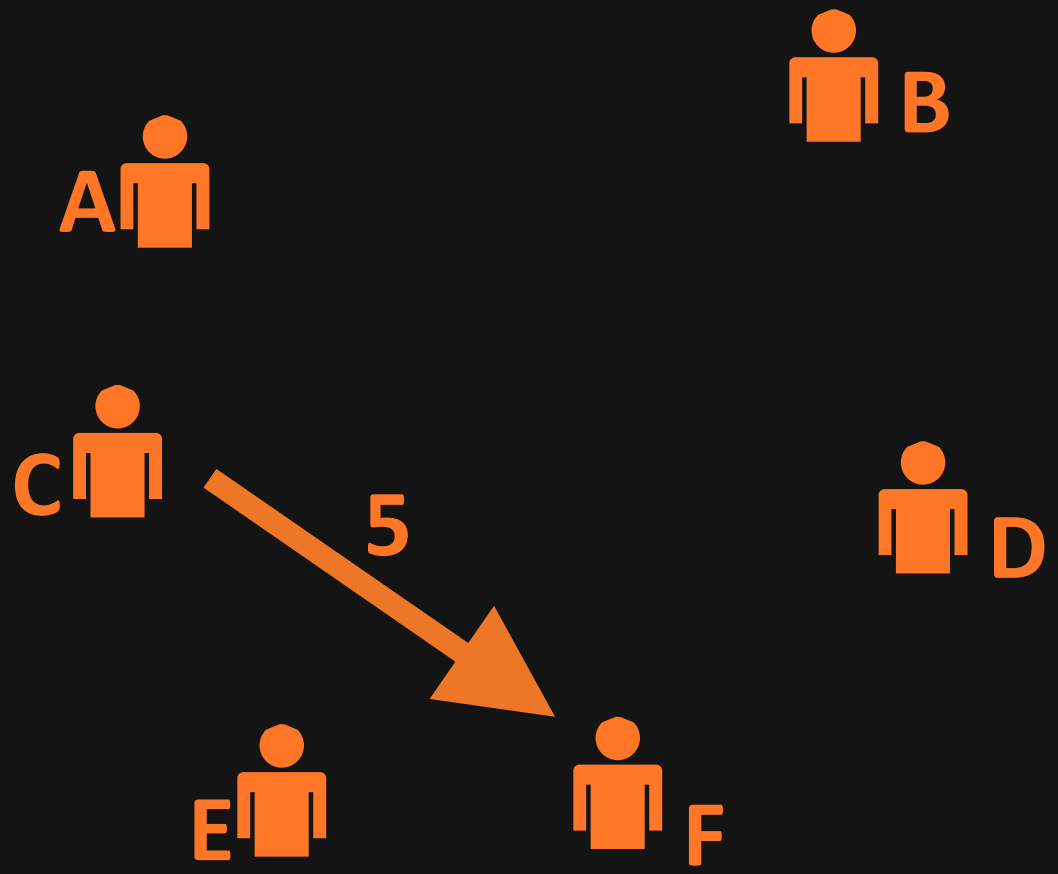
Rejestr pożyczek



Grupa znajomych

5d825022bd617f7a

C → F, 5



Rejestr pożyczek

Grupa znajomych

5d825022bd617f7a

C → F, 5

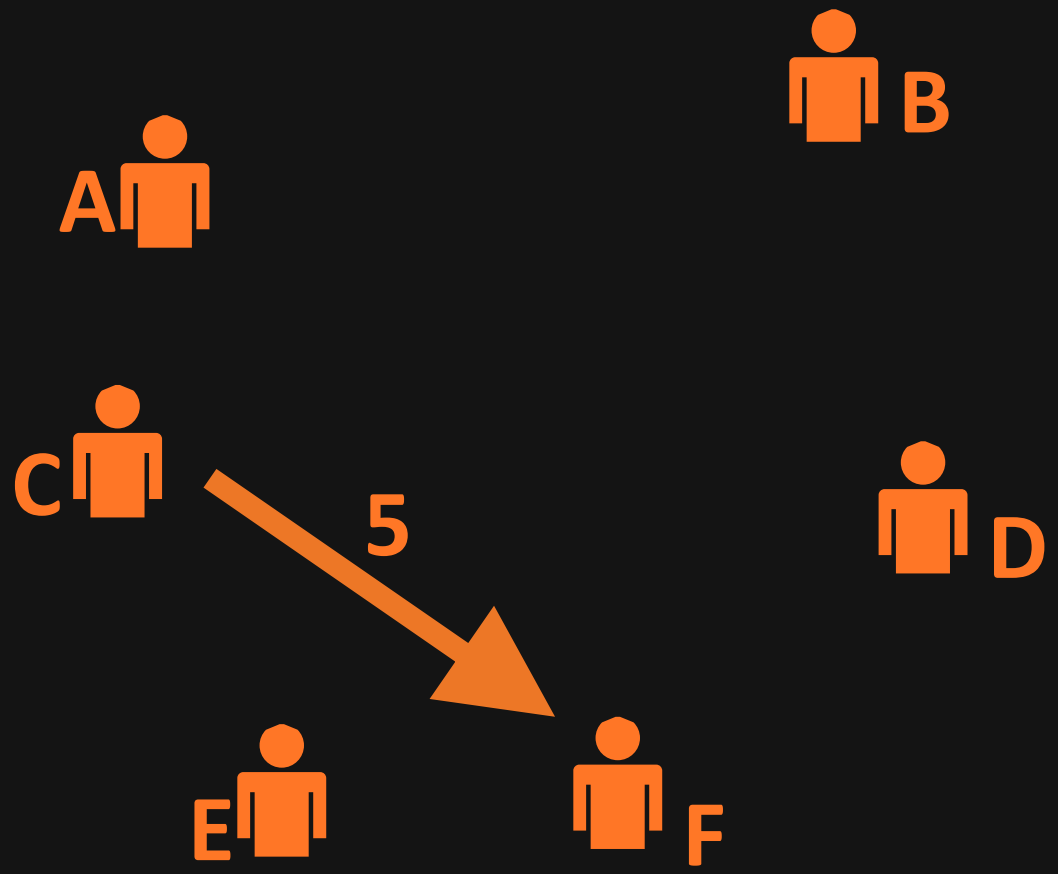
… → …, …

… → …, …

… → …, …

… → …, …

Rejestr pożyczek



Grupa znajomych

5d825022bd617f7a

C → F, 5

… → …, …

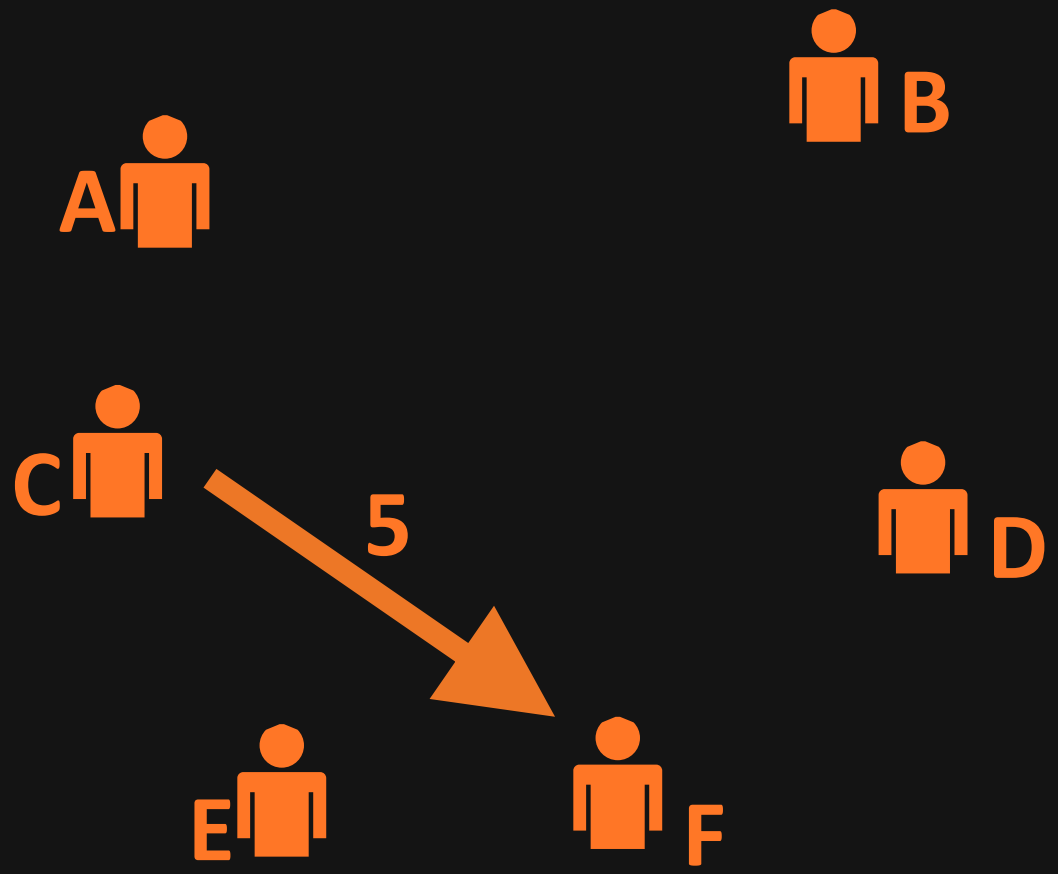
… → …, …

… → …, …

… → …, …

3f57257276241b16

Rejestr pożyczek



Grupa znajomych

3f57257276241b16

… → …, …

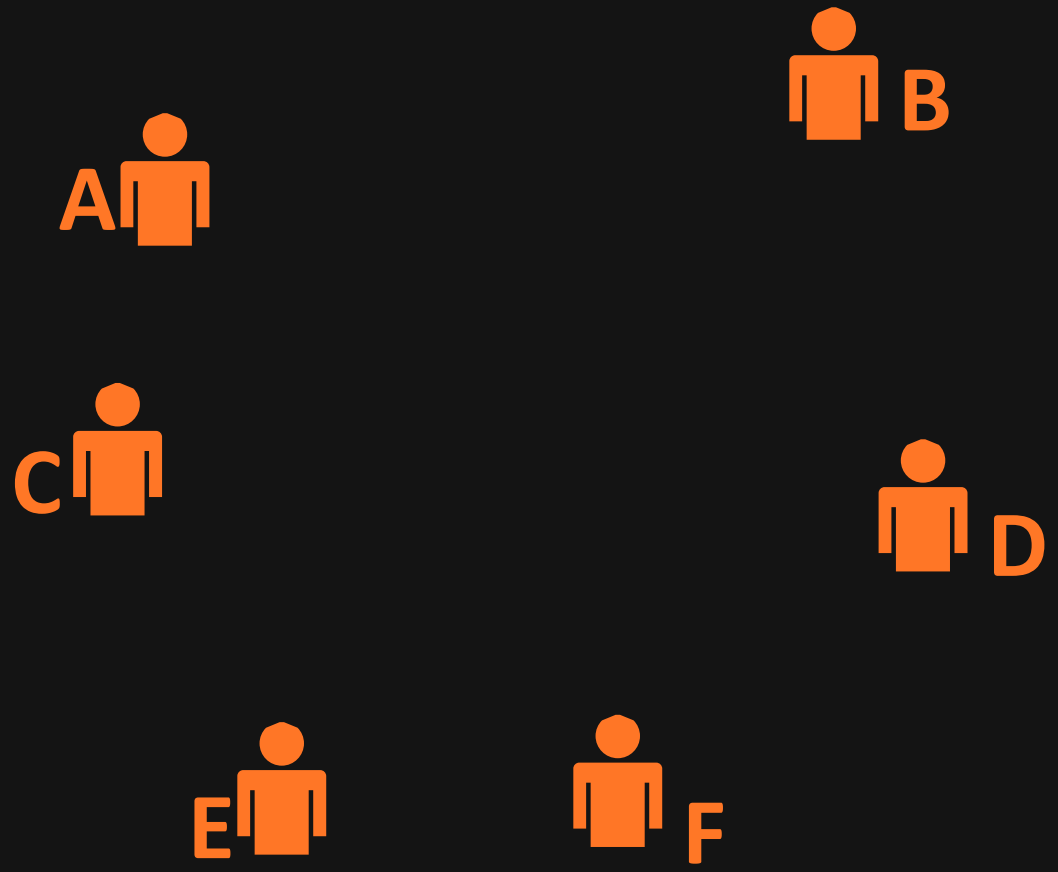
… → …, …

… → …, …

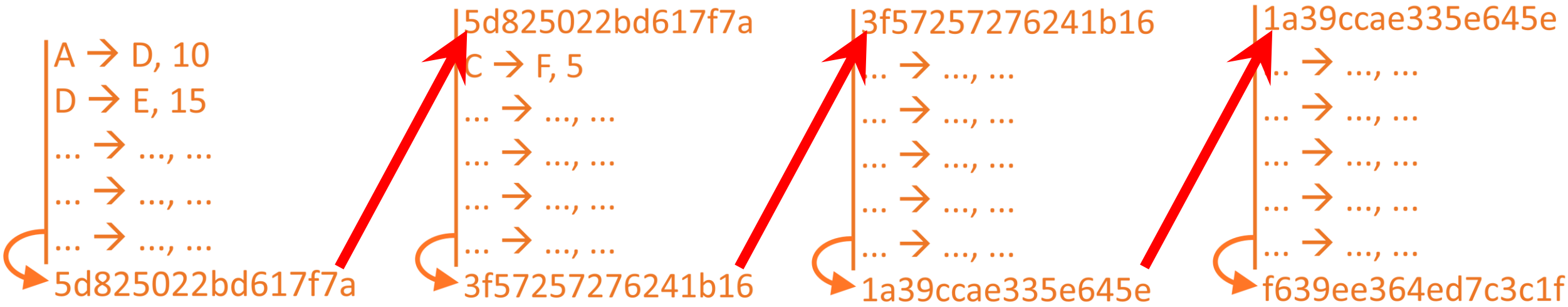
… → …, …

… → …, …

Rejestr pożyczek

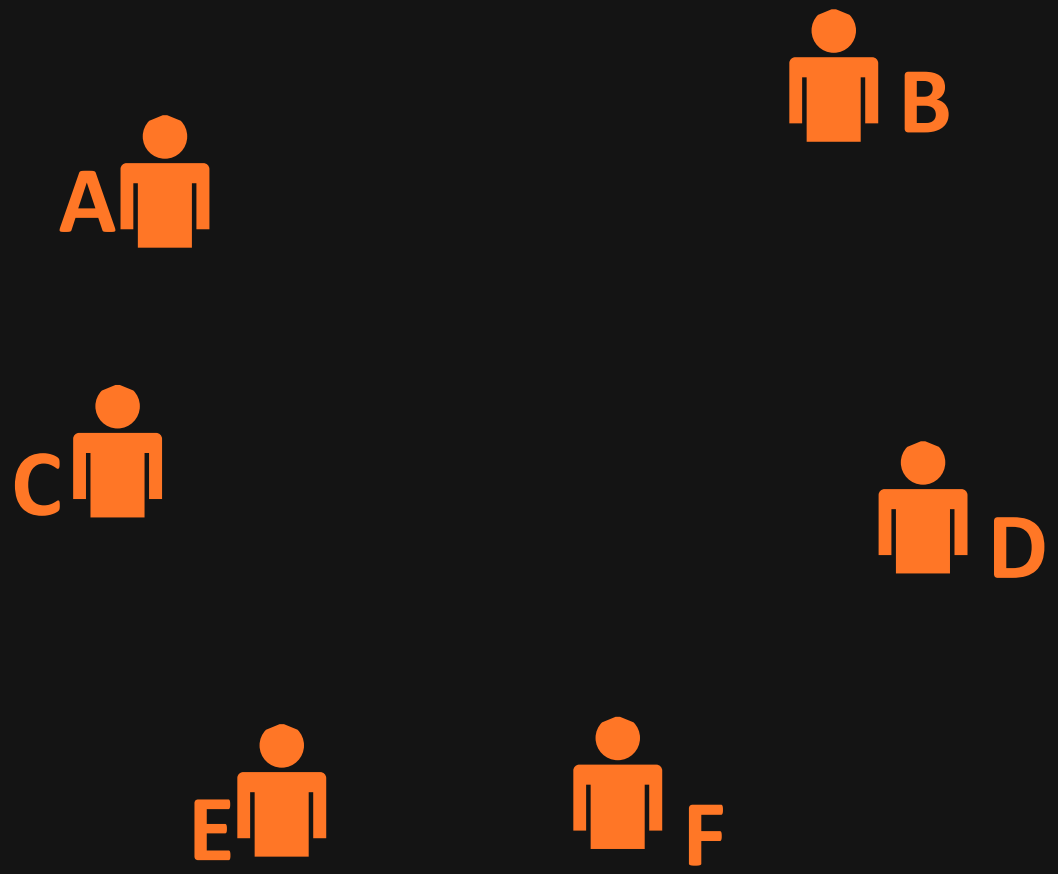


Grupa znajomych


A → D, 10
D → E, 15
… → …, …
… → …, …
… → …, …
5d825022bd617f7a
5d825022bd617f7a
C → F, 5
… → …, …
… → …, …
… → …, …
… → …, …
3f57257276241b16
3f57257276241b16
… → …, …
… → …, …
… → …, …
… → …, …
… → …, …
1a39ccae335e645e
1a39ccae335e645e
… → …, …
… → …, …
… → …, …
… → …, …
… → …, …
f639ee364ed7c3c1f

Przychodzi nowy sąsiad i chce dołączyć do grupy znajomych. Co teraz?

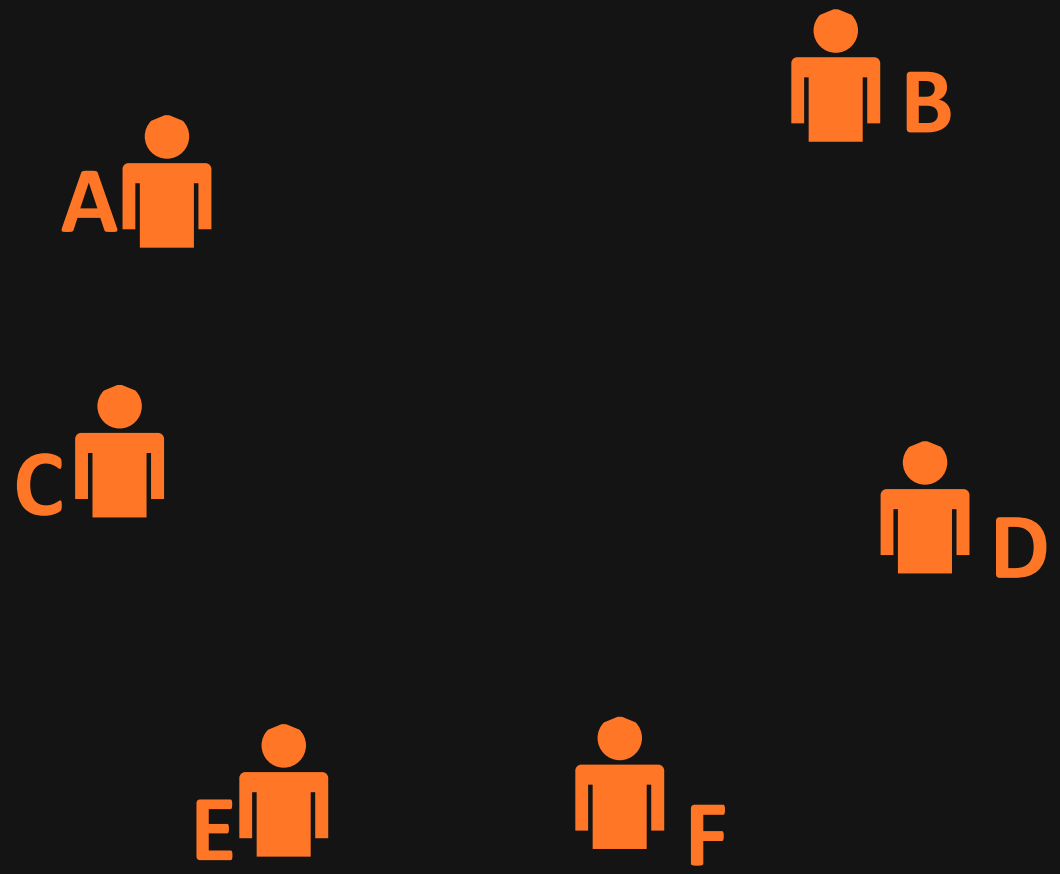
Rejestr pożyczek



Grupa znajomych

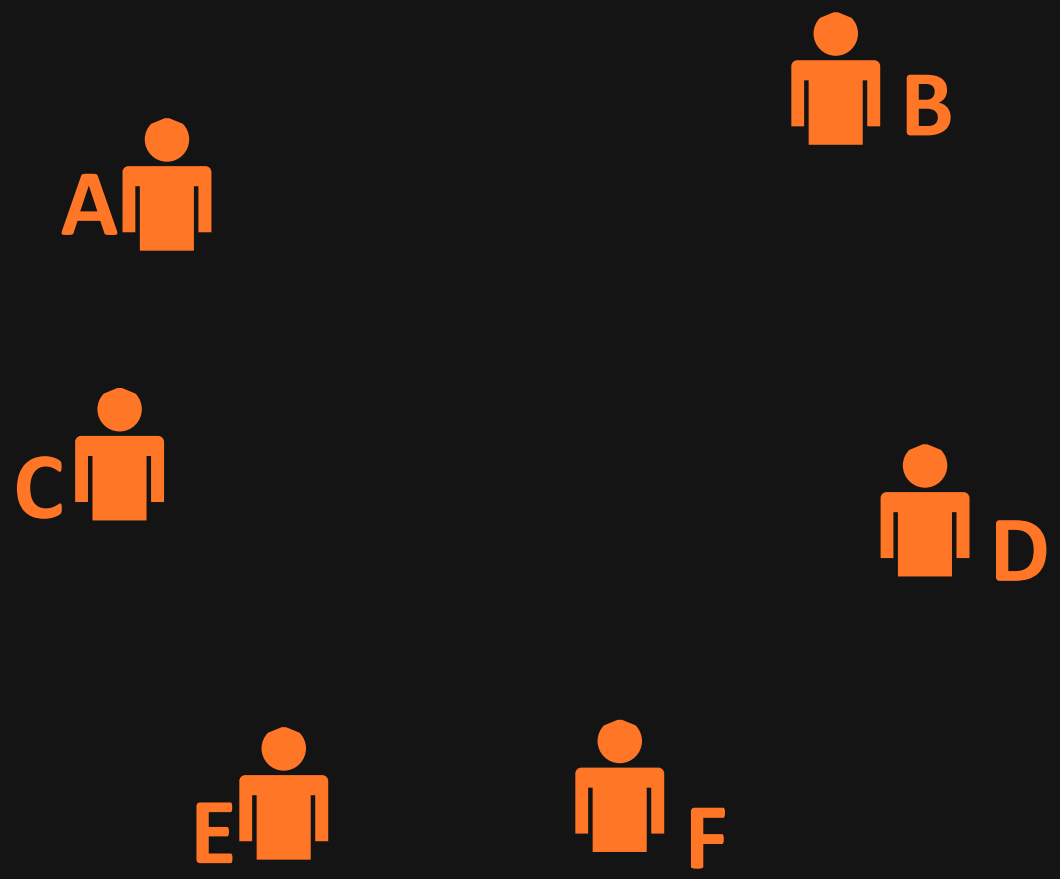
Jak to skalować?

Rejestr transakcji



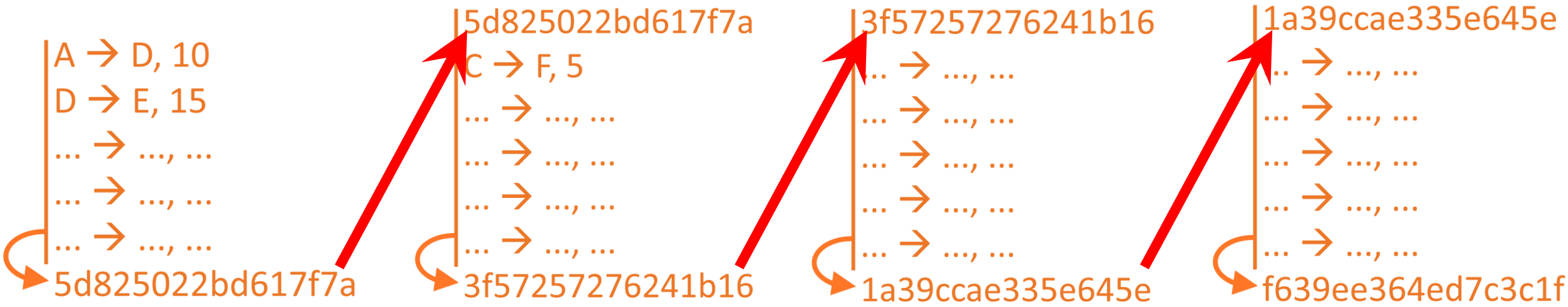
Dziesięć milionów obcych ludzi

Peer-to-peer



Rejestr transakcji

Dziesięć milionów obcych ludzi



- Pierwszy typ komunikatu to „oto nowa transakcja”
- Sieci P2Ps są zawodne, nie mamy gwarancji kolejności powiadamiania
- Kartki nie skończą się wszystkim naraz, więc drugim typem komunikatu będzie „oto pełna zawartość kolejnej kartki (bloku) i jej skrót”

Rozproszony rejestr

Kropki zaczynają się łączyć:

- Mamy sieć P2P
- Każdy węzeł sieci przechowuje kompletny zapis blockchaina
- Każdy blok zawiera skrót (hasz) poprzedniego bloku

- W każdym bloku są transakcje (?)

Kryptografia klucza publicznego

kryptografia asymetryczna

slido.com
#76766

Kryptografia klucza publicznego

Chcemy szyfrować dane jednym hasłem a rozszyfrować innym.

Chcemy szyfrować dane jednym kluczem a rozszyfrować innym.

Kryptografia klucza publicznego

Wybieramy sobie bardzo dużą liczbę, najlepiej poprzez losowanie, aby na pewno nikt jej nie odgadł. Przykład: kostka sześcienna, parzyste to zero, nieparzyste to jeden, rzucamy 256 razy, spisujemy wyniki.

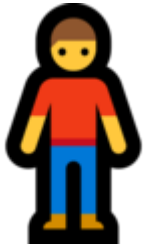
Wylosowaliśmy liczbę z przedziału od zera do 115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936.

To bardzo duża liczba.

Atomów we Wszechświecie jest niewiele więcej.

Kryptografia klucza publicznego

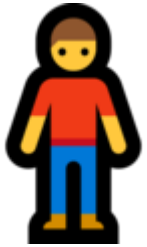
Do tej bardzo dużej liczby dobieramy w szczególny sposób inną bardzo dużą liczbę. Od tej pory na te liczby będziemy mówić „klucze”.



Pierwsza liczba to klucz prywatny i to ma być ścisła tajemnica.

Druga liczba to klucz publiczny i ona ma być znana każdemu, możemy ją wykrzykiwać na rynku albo umieścić na wizytówkach.

Kryptografia asymetryczna!

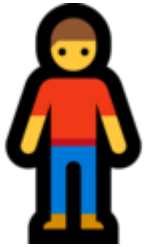


Kluczem prywatnym możemy coś zaszyfrować.

Kluczem publicznym możemy to odszyfrować.

(jeśli odszyfrowanie się uda, to wiemy, że wiadomość zaszyfrował posiadacz klucza prywatnego)

Podpisy cyfrowe



Podpisujemy coś kluczem prywatnym

- Bierzemy tekst transakcji i obliczamy jego skrót
- Szyfrujemy skrót, dostajemy podpis

Weryfikujemy podpis kluczem publicznym

- Bierzemy tekst transakcji i obliczamy jego skrót
- Odszyfrowujemy podpis
- Patrzymy, czy skrót i odszyfrowany podpis są identyczne

Kluczowa (hehe) informacja

Jeśli patrzymy na:
– tekst
– podpis cyfrowy
– klucz publiczny,

to potrafimy sprawdzić, czy podpis pod tekstem został sporządzony kluczem prywatnym powiązanym z tym kluczem publicznym, na który patrzymy.

- Funkcja skrótu (funkcja haszująca)
- **Blockchain**
- Sieci P2P
- **Rozproszony rejestr**
- Kryptografia klucza publicznego
- **Generowanie jednostek kryptowaluty**
- Regulacja trudności tworzenia bloków
- **Konsensus i proof of work**
- Co to jest kopalnia i czym się kopie bitcoiny
- Do czego komu Bitcoin i kto to w ogóle wymyślił
- Zastosowania blockchaina (buhahahahahahaha)

Jesteśmy tutaj i zaraz wszystkie informacje połączą się w jedną całość czyli Bitcoina

slido.com
#76766

Nareszcie bitcoin!

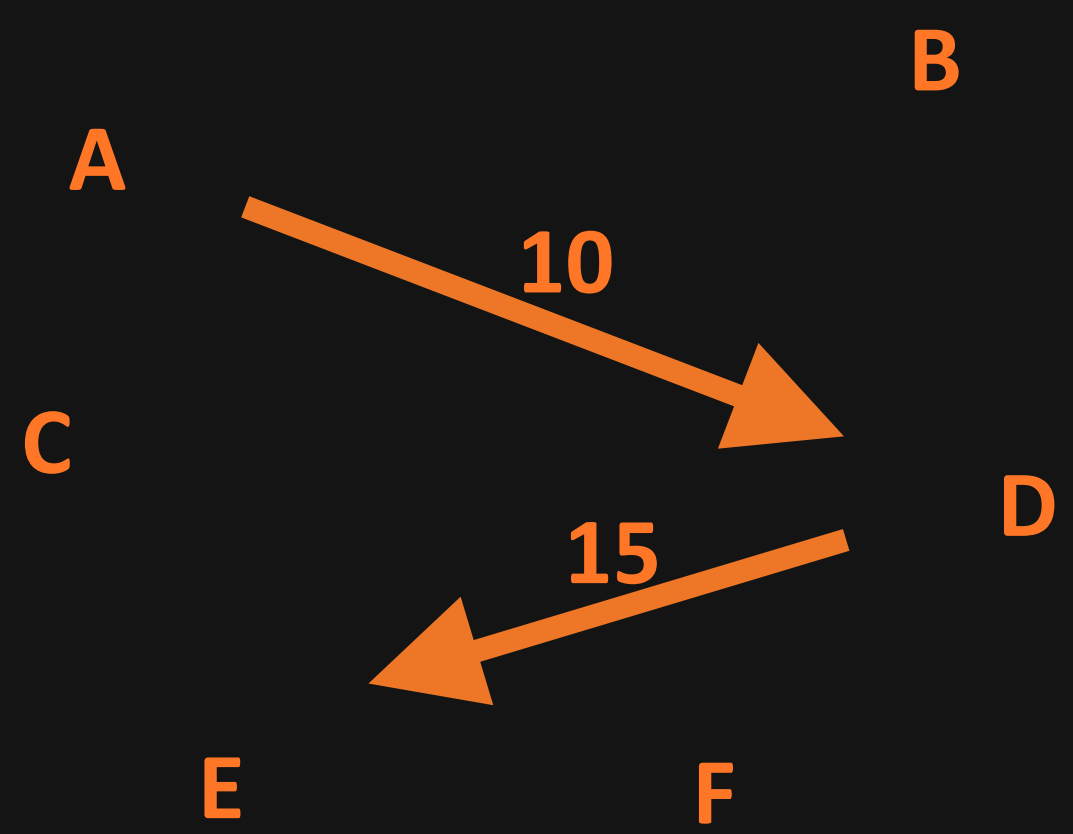
Uwaga, nadchodzą śmiertelnie niebezpieczne uproszczenia!

Klucz publiczny to „bitcoinowy numer konta” albo „adres portfela”. Od tej pory będziemy mówić o „kluczu prywatnym” i „adresie”.

Pamiętacie ten obrazek?

A, B, C… – to są adresy (klucze publiczne)

Rejestr pożyczek

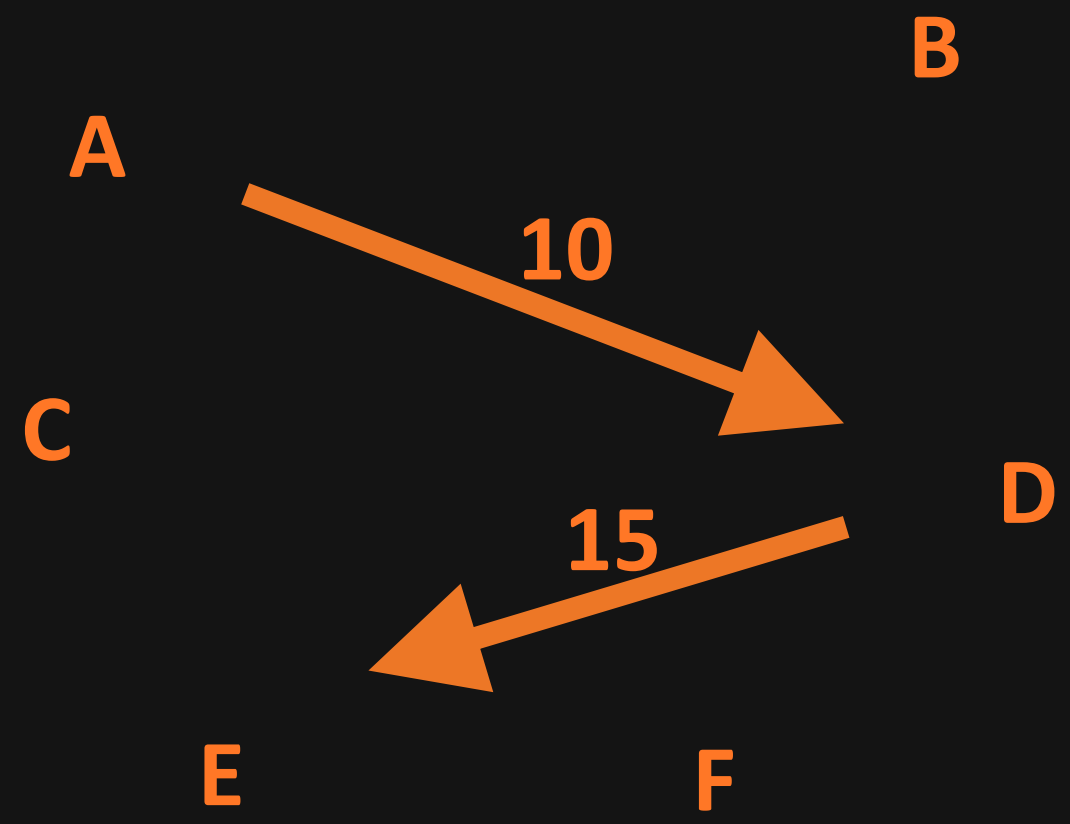


Grupa znajomych

Transakcja to polecenie przekazania środków z jednego adresu na inny.

Transakcja musi być podpisana.

Rejestr pożyczek

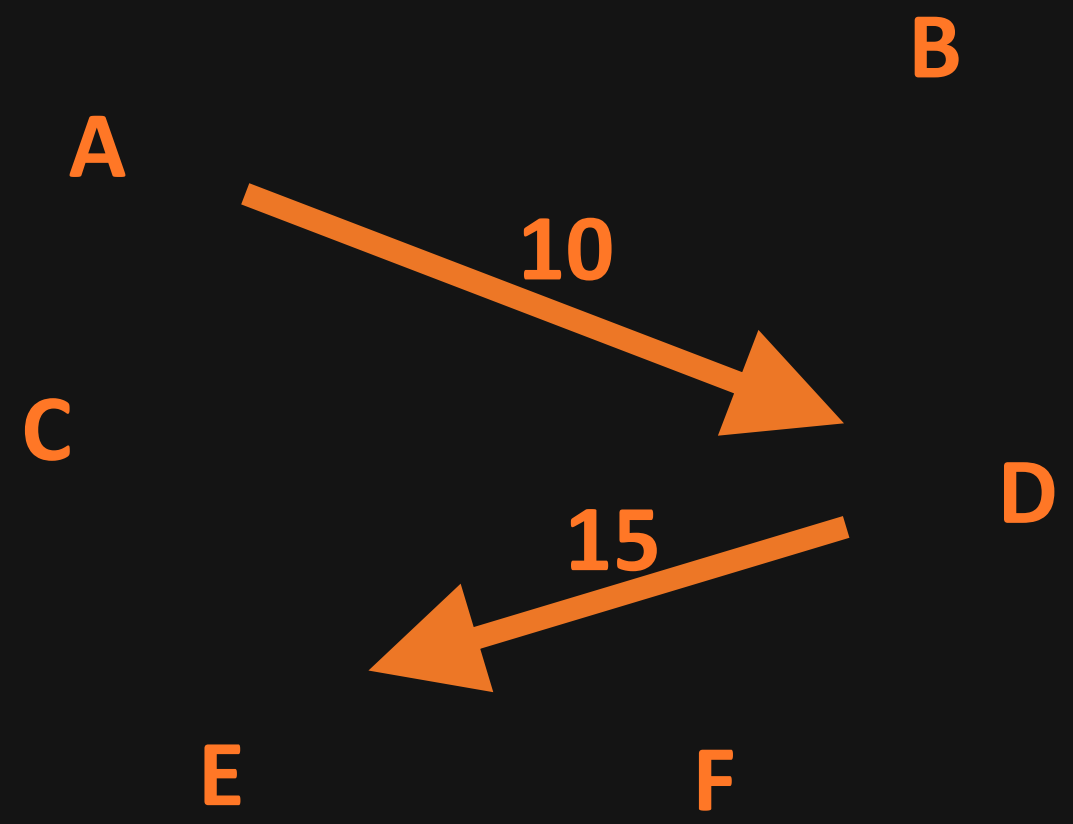


Grupa znajomych

Aby przekazać gdzieś środki, potrzebujemy jedynie adresu portfela docelowego.

Aby zlecić transakcję, potrzebujemy klucza prywatnego do portfela nadawcy.

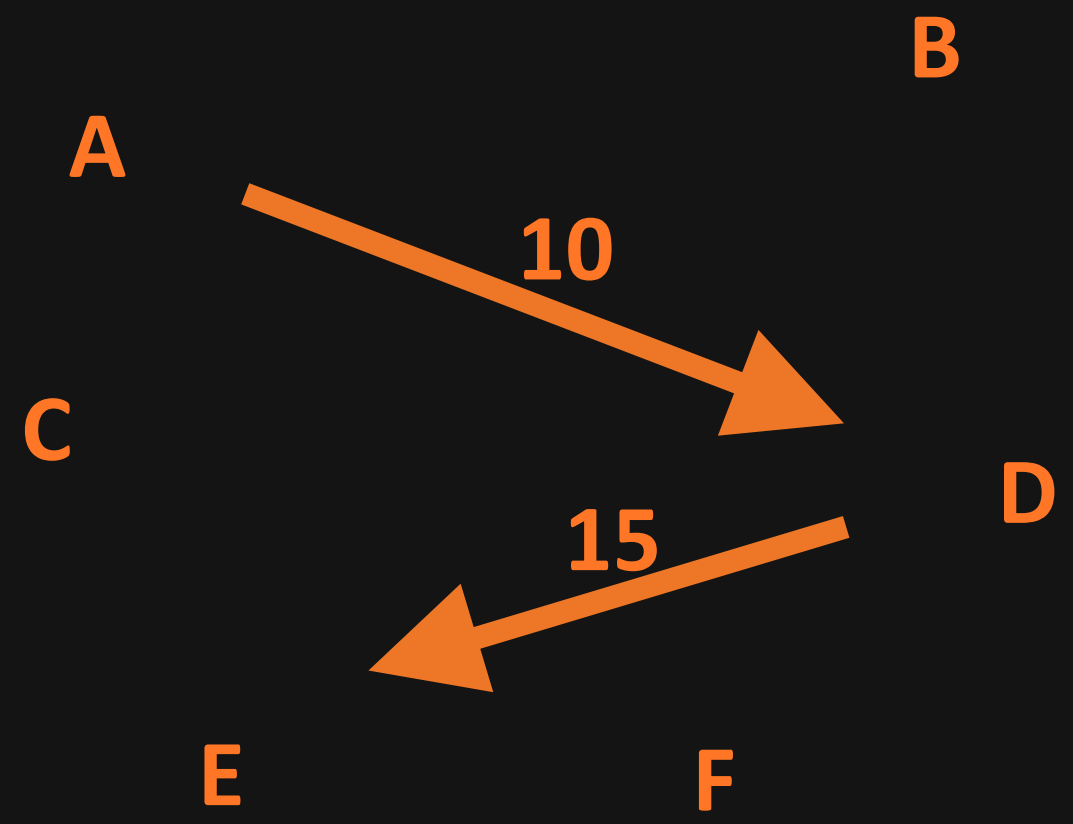
Rejestr pożyczek



Grupa znajomych

Szczegół techniczny nr 1: jedna transakcja może dzielić środki na wiele adresów.

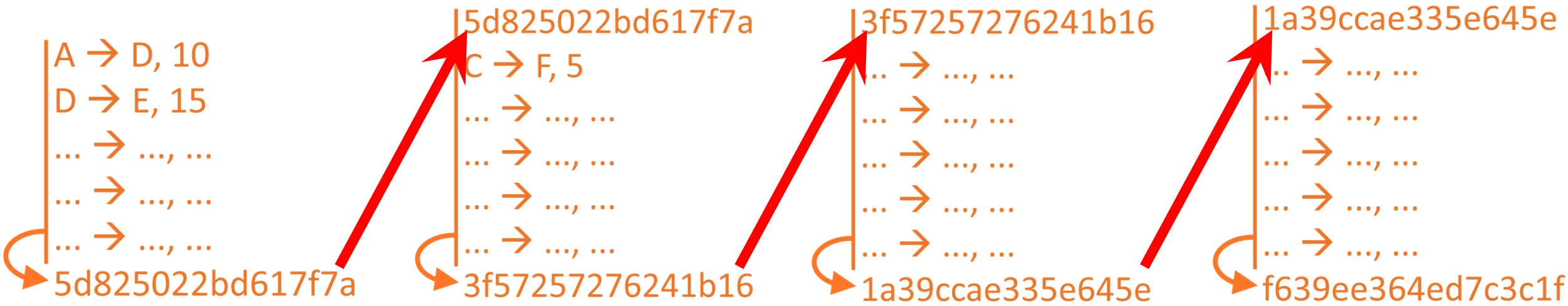
Szczegół techniczny nr 2: jedna transakcja może łączyć środki z wielu adresów, potrzebuje do tego wielu podpisów.



Rejestr pożyczek

Grupa znajomych

Co wiemy do tej pory



- każda transakcja w każdym bloku to przekazanie środków z jednego adresu na inny adres; nie rejestrujemy nigdzie „bieżącego stanu konta”
- jeśli prześledzimy całego blockchaina od samego początku to dowiemy się, które portfele mają saldo większe od zera

Bitcoin

Kryptowaluta i system płatności oparty na technologii blockchain działającej w sieci P2P

bitcoin

jednostka monetarna sieci Bitcoin

(100.000.000 satoshi)

Generowanie bitcoinów

czyli skąd się biorą nowe jednostki

slido.com
#76766

900 tys. zł


BITCOIN • DIGITAL • DECENTRALIZED • PEER TO PEER
1 TROY OZ 999 FINE COPPER .999 MONETARY METALS

Skąd się biorą nowe bitcoiny

W każdym bloku może znaleźć się transakcja przekazująca 6.25 BTC z adresu „0” na dowolny inny adres. Jest to główna zachęta do tworzenia nowych bloków, kwota ta stanowi nagrodę dla „górnika”.

Na początku istnienia Bitcoina premia wynosiła 50 BTC, co kilka lat wartość ta zmniejsza się o połowę (aż do 0.00000001 około roku 2136).

Łącznie wykopanych zostanie 21 milionów bitcoinów. Do tej pory w obieg wprowadzono około 88.5% tej liczby. Nie wiadomo, ile przepadło.

Zachęta nr 2

Fees (Satoshis PER BYTE)	Unconfirmed transactions / Transactions today (# OF TRANSACTIONS IN MEMPOOL IN LAST 336 HOURS / # OF TRANSACTIONS IN LAST 24 HOURS)	Delay ESTIMATED IN BLOCKS	Time ESTIMATED IN MINUTES
0	0 / 36	21-Inf	240-Inf
1-30	23889 / 24682	5-Inf	50-Inf
31-60	7129 / 7779	5-Inf	50-Inf
61-90	4683 / 5083	5-Inf	45-Inf
91-120	4304 / 4869	5-Inf	45-Inf
121-150	5442 / 6449	5-141	45-2100
151-180	5814 / 6747	5-124	45-1800
181-210	4644 / 6185	3-100	20-1380
211-240	2838 / 6694	1-42	0-600
241-270	847 / 14158	0-29	0-480
271-300	717 / 16337	0-18	0-360
301-330	609 / 27658	0-13	0-240
331-360	432 / 23444	0-10	0-180
361-390	384 / 32817	0-4	0-80
391-420	222 / 28960	0-1	0-55
421-450	189 / 33201	0	0-45
451-480	64 / 13800	0	0-45
481-510	52 / 6356	0	0-45
511+	166 / 27574	0	0-45

140 tys. zł

https://bitcoinfees.earn.com/

Chciwość!

Aby cała sieć Bitcoina działała, ktoś musi formować nowe bloki.

Górnicy chcą zarabiać jak najwięcej, więc włączają do bloków transakcje z najwyższymi prowizjami.

Efekt – mamy nowe bloki z transakcjami.

Wiemy już, jak działają „przelewy”

- Tworzymy nową transakcję i podpisujemy ją kluczem prywatnym; w transakcji mamy: adres źródłowy, adres docelowy, kwotę i prowizję
- Wysyłamy transakcję do sieci P2P, trafia ona do puli transakcji
- Górnicy próbują sformować najbardziej opłacalne transakcje w bloki w taki sposób, aby blok był prawidłowy
- Gdy blok zostanie sformowany a nasz „przelew” będzie w nim zawarty, transakcja jest przeprowadzona

…ale nie na pewno!

Regulacja trudności

nowy blok co 10 minut

slido.com
#76766

Chętnych na prowizję jest wielu

- Założenie - nowy blok ma się pojawiać co 10 minut
- Potrzebujemy sposobu na to, by każdy chętny miał równe szanse na utworzenie bloku, mechanizm musi być autonomiczny i niezależny od czyjejkolwiek manipulacji
- Proof of Work

Funkcja skrótu powraca

Litwo, ojczyzno moja
5d825022bd617f7ab3b773ef37f75ec475a1905308db0fb91050ed24065ba2e1

Litwo, ojczyzno moja4
058f5174895e9d2b8d373d84cb05803b98a93e0004c7eec3b42520bb92561b32

Litwo, ojczyzno moja709
006560af9a9d46deb2eee3ddeb10dd2001064406ecacea797f61f76c46f71260

Litwo, ojczyzno moja142
000baf3390413cc6a3fbe805625c97ff6733b71891eb47d0cca24802c986bbb1

Funkcja skrótu powraca

Litwo, ojczyzno moja
5d825022bd617f7ab3b773ef37f75ec475a1905308db0fb91050ed24065ba2e1

Litwo, ojczyzno moja4
058f5174895e9d2b8d373d84cb05803b98a93e0004c7eec3b42520bb92561b32

Litwo, ojczyzno moja709
006560af9a9d46deb2eee3ddeb10dd2001064406ecacea797f61f76c46f71260

Litwo, ojczyzno moja142
000baf3390413cc6a3fbe805625c97ff6733b71891eb47d0cca24802c986bbb1

Bieżąca trudność

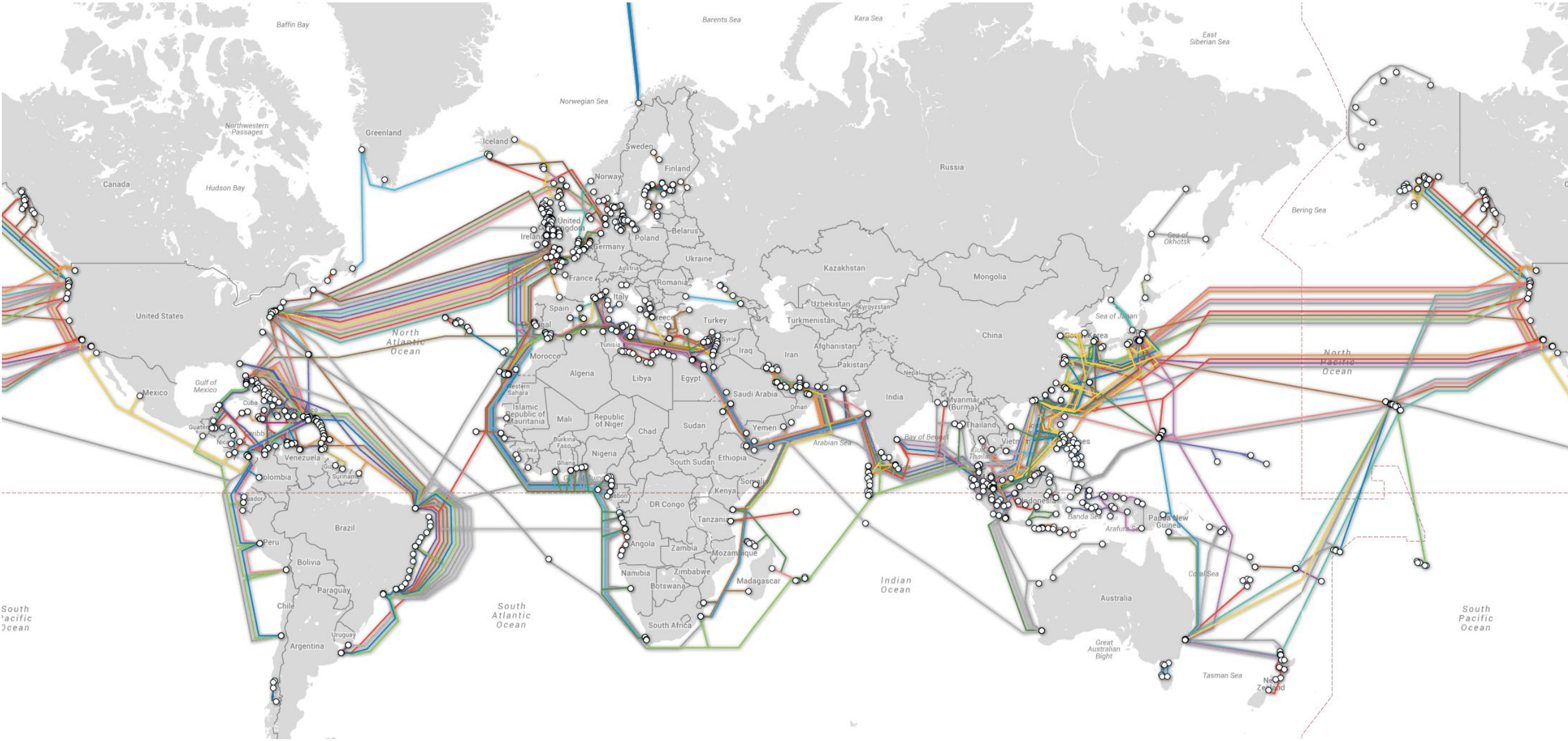
- Blok 665617 z 11 stycznia 2021 ma skrót **000000000000000000010e30b25906a3b85c8995e84d396fff26242d9e4556ca**
- 19 zer wiodących, trudność spełniana przez jeden na 75.557.863.725.914.323.419.136 (75 tryliardów / sekstylionów) haszy

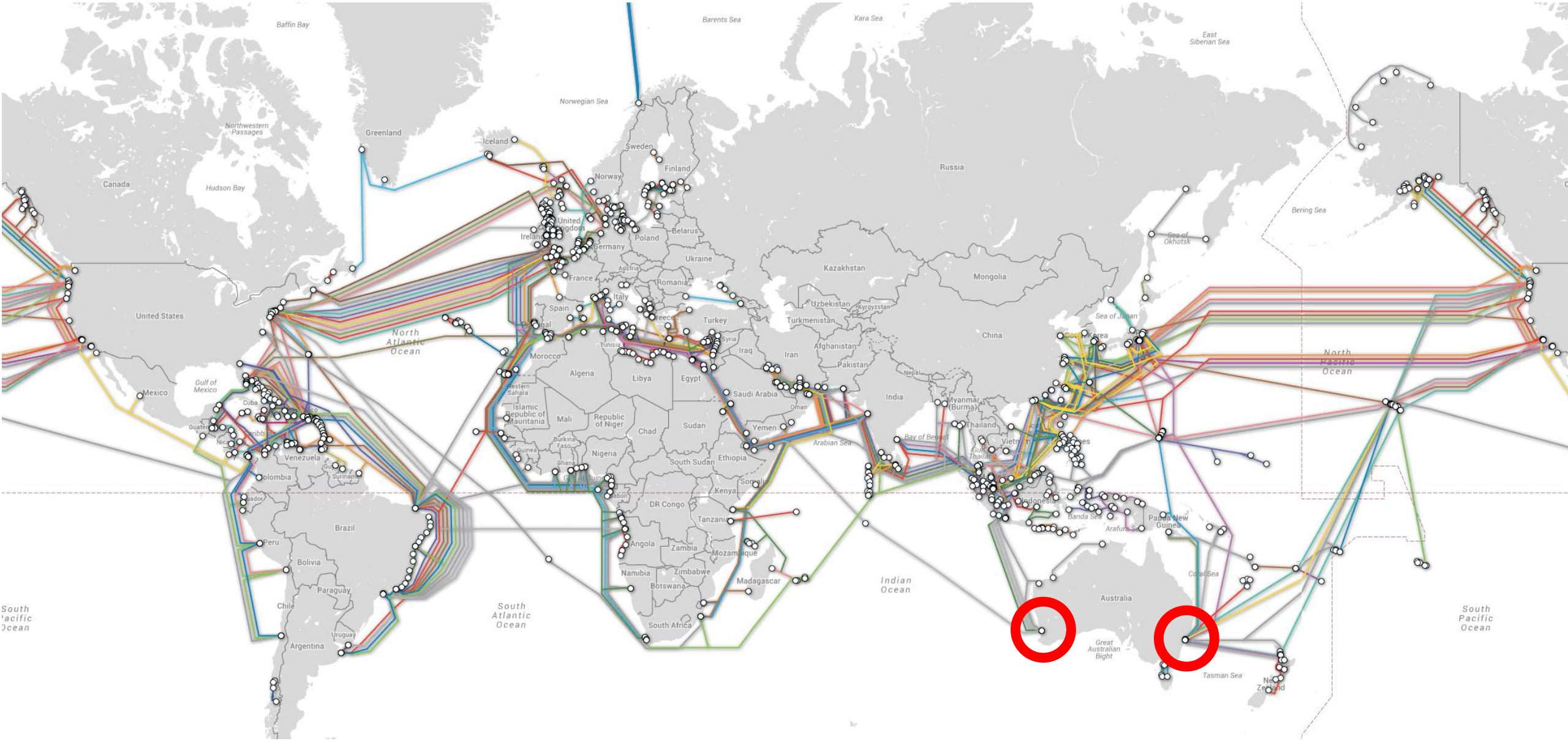
- Trudność jest adjustowana automatycznie przez protokół co około dwa tygodnie

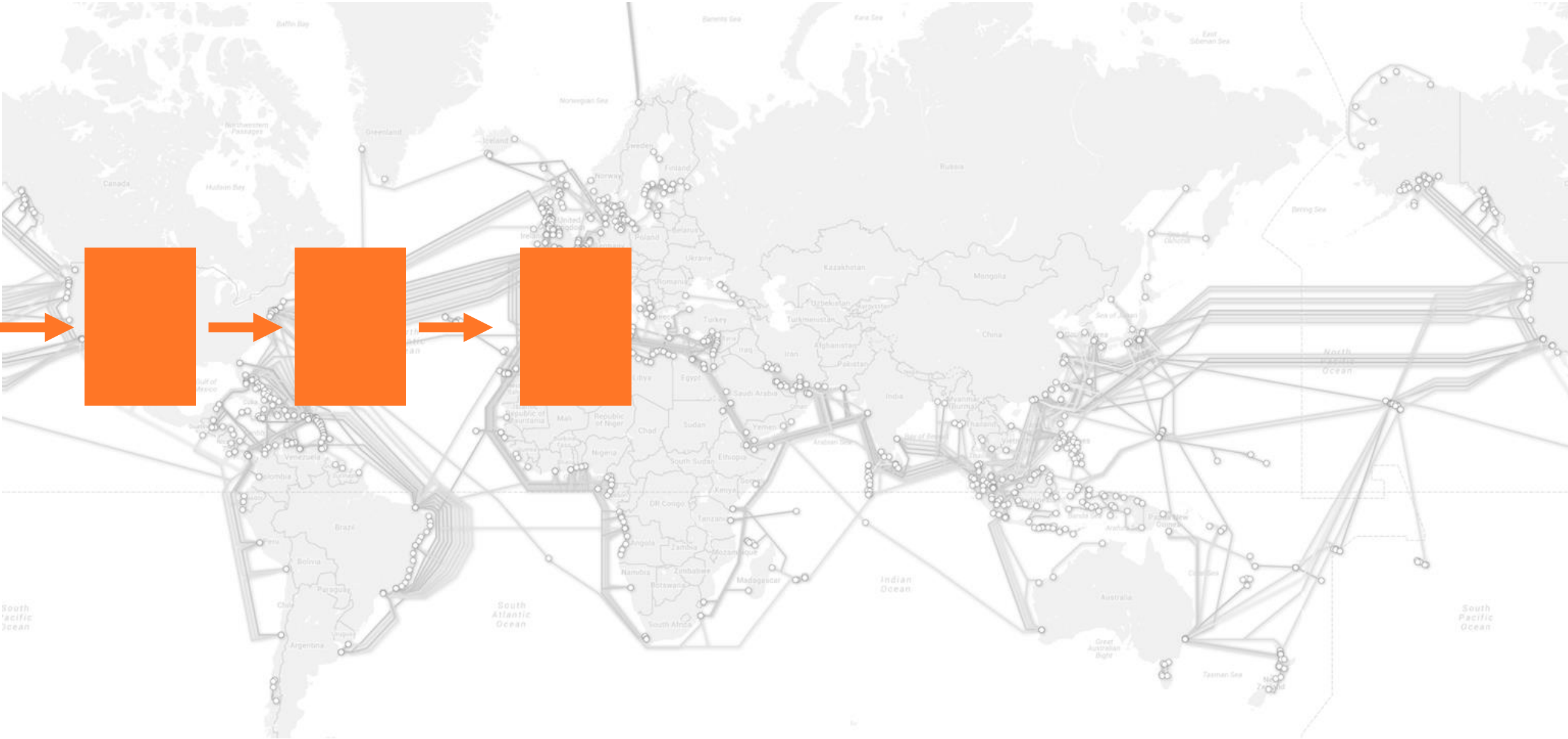
Konsensus

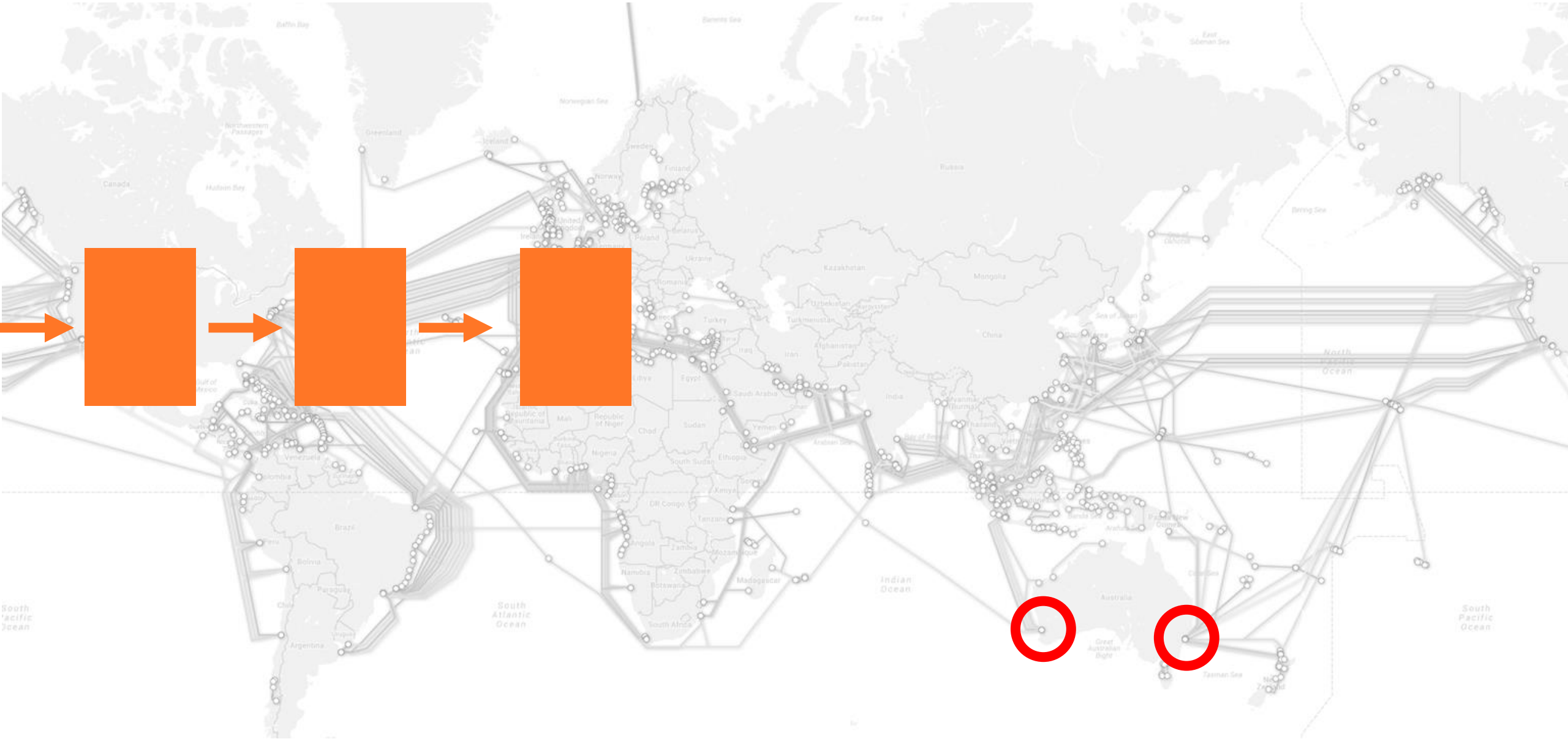
oraz Proof of Work

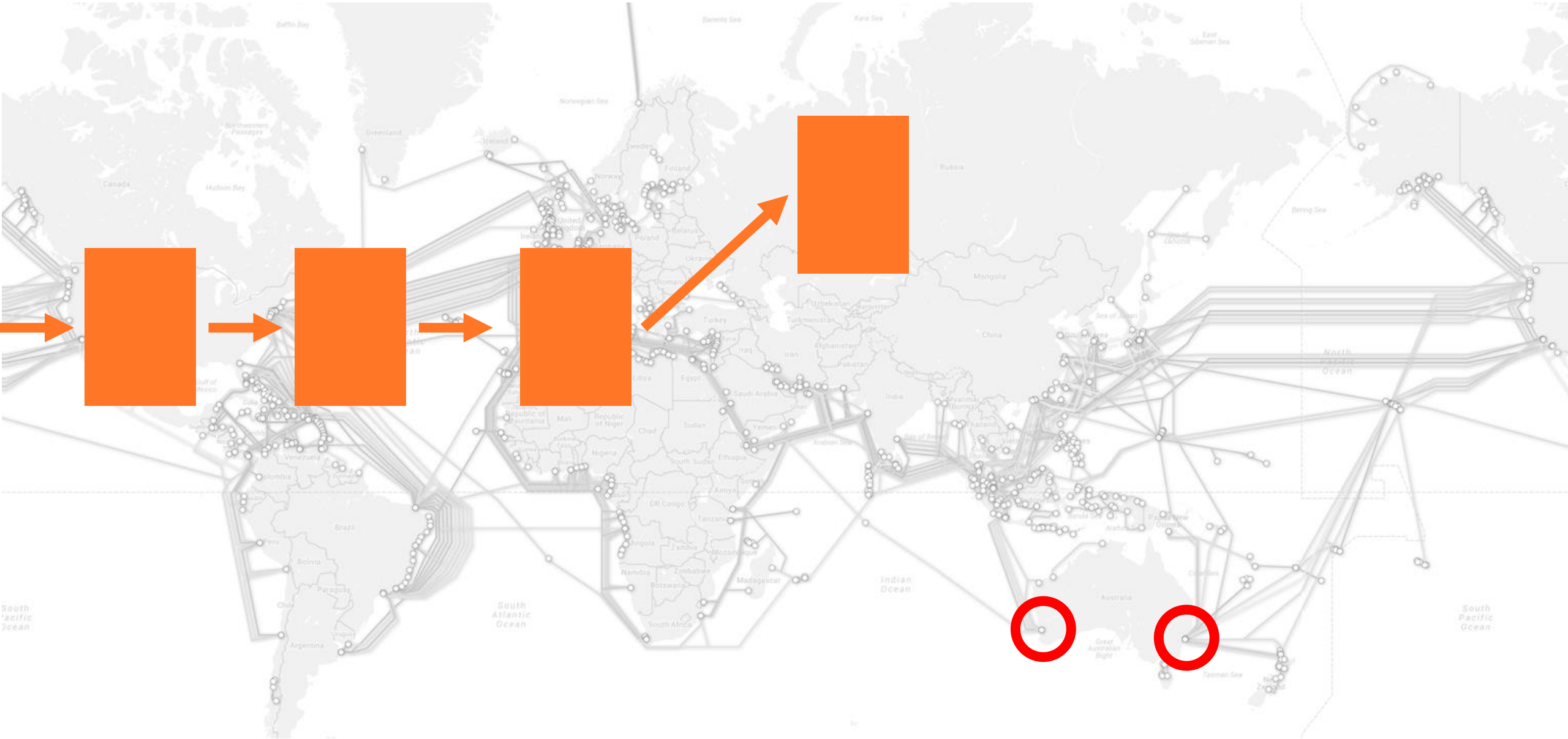
slido.com
#76766

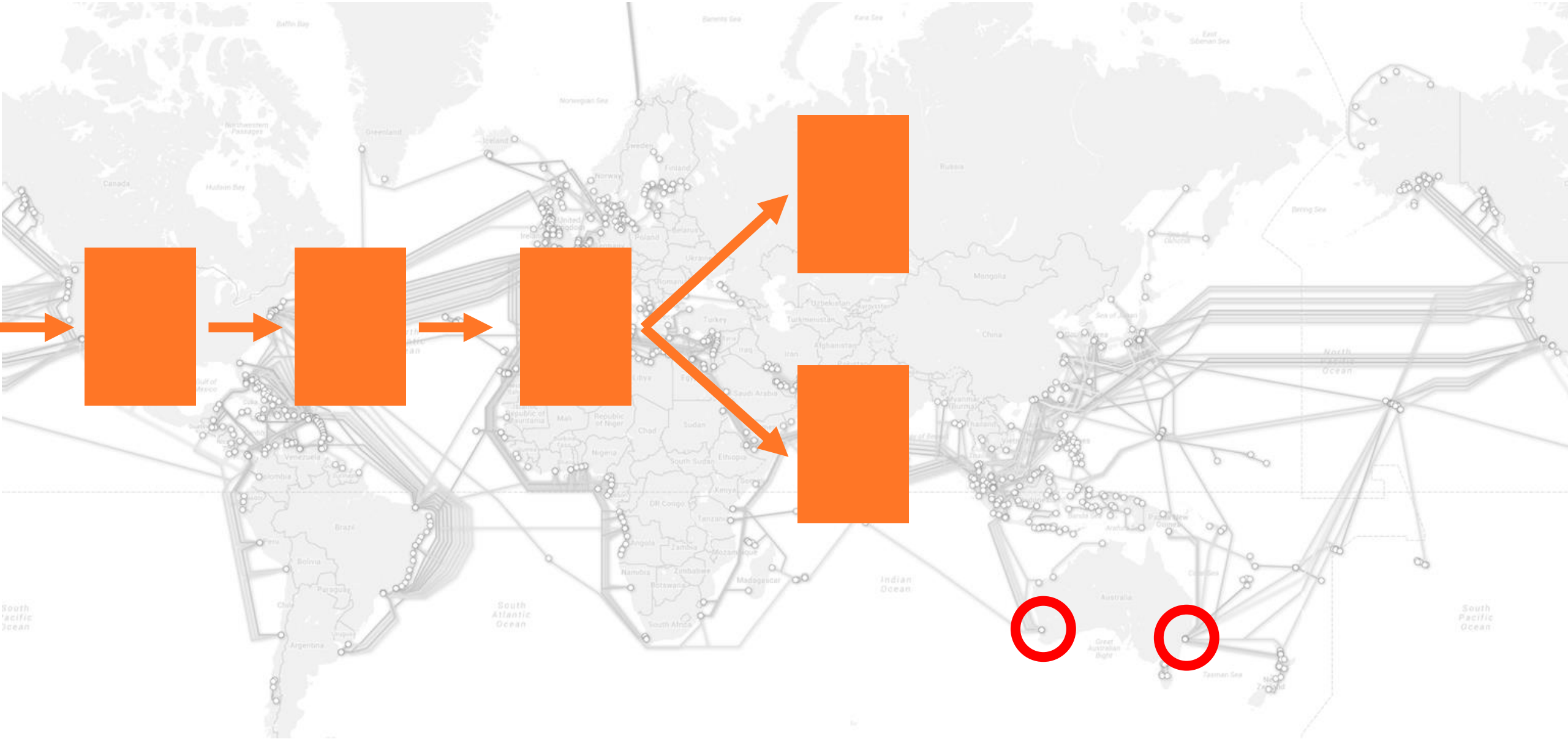

Baffin Bay
Barents Sea
Kara Sea
East Siberian Sea
Norwegian Sea
Northwestern Passages
Greenland
Iceland
Canada
Hudson Bay
Sweden
Finland
Norway
Russia
Bering Sea
United Kingdom
Ireland
Germany
Poland
Belarus
Ukraine
Sea of Okhotsk
Kazakhstan
Mongolia
France
Austria
Romania
Italy
Spain
Uzbekistan
Kyrgyzstan
Turkmenistan
Sea of Japan
China
United States
North Atlantic Ocean
Turkey
Syria
Iraq
Iran
Afghanistan
Pakistan
Morocco
Algeria
Libya
Egypt
Saudi Arabia
Nepal
India
North Pacific Ocean
Gulf of Mexico
Mexico
Western Sahara
Islamic Republic of Mauritania
Mali
Republic of Niger
Chad
Sudan
Yemen
Oman
Arabian Sea
Bay of Bengal
Myanmar (Burma)
Thailand
Nigeria
Ethiopia
South Sudan
Somalia
Kenya
Venezuela
Colombia
Brazil
Peru
Bolivia
Paraguay
Chile
Argentina
Uruguay
DR Congo
Tanzania
Angola
Zambia
Mozambique
Namibia
Zimbabwe
Botswana
Madagascar
South Africa
Indian Ocean
Indonesia
Banda Sea
Papua New Guinea
Coral Sea
Australia
Great Australian Bight
Tasman Sea
New Zealand
South Pacific Ocean
South Atlantic Ocean

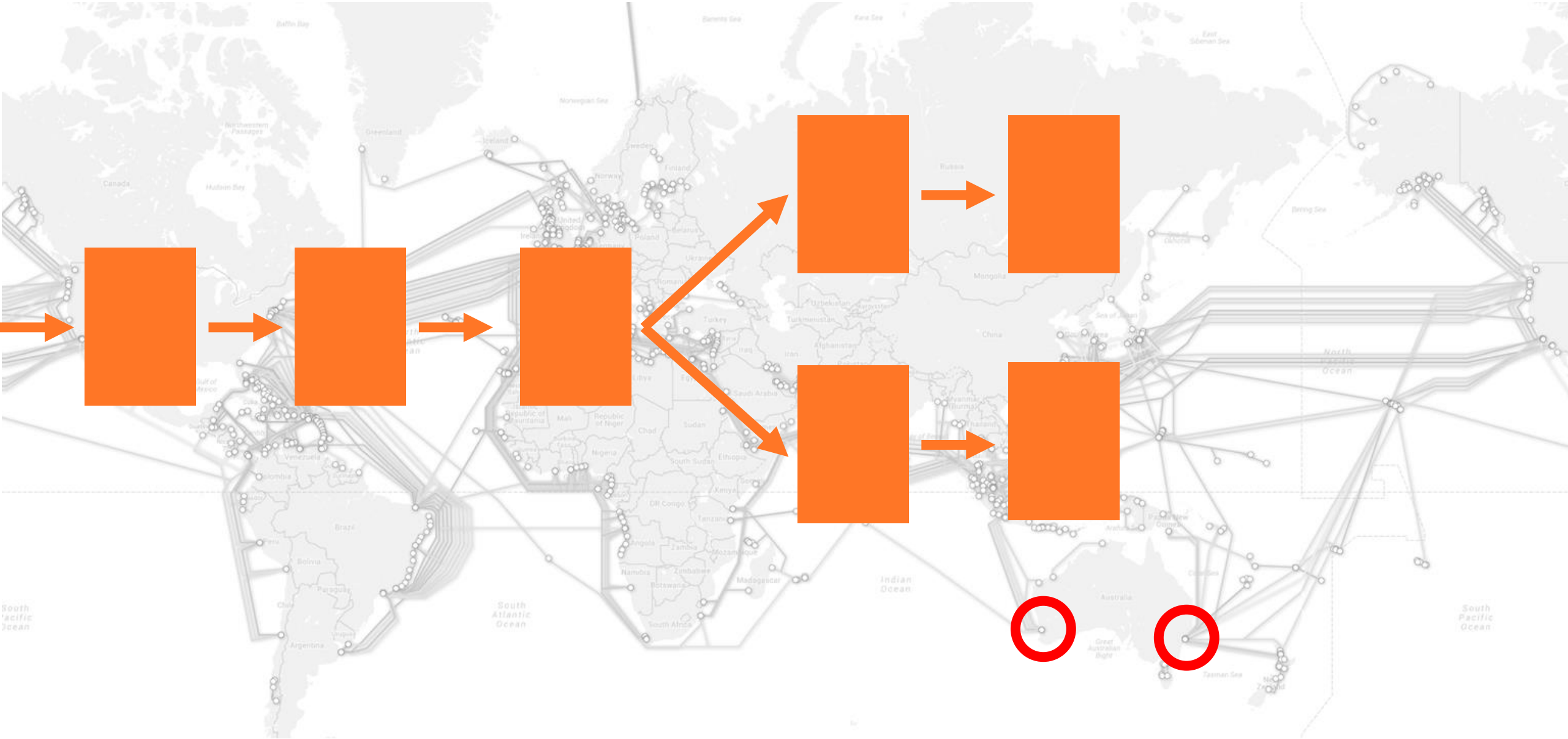

Baffin Bay
Barents Sea
Kara Sea
East Siberian Sea
Norwegian Sea
Northwestern Passages
Greenland
Iceland
Canada
Hudson Bay
Sweden
Finland
Norway
Russia
Bering Sea
United Kingdom
Ireland
Germany
Poland
Belarus
Ukraine
Sea of Okhotsk
Kazakhstan
Mongolia
France
Austria
Romania
Uzbekistan
Kyrgyzstan
Turkmenistan
Sea of Japan
China
United States
North Atlantic Ocean
Spain
Italy
Greece
Turkey
Syria
Iraq
Iran
Afghanistan
Pakistan
Nepal
India
North Pacific Ocean
Morocco
Algeria
Libya
Egypt
Saudi Arabia
Oman
Yemen
Arabian Sea
Bay of Bengal
Myanmar (Burma)
Thailand
Mexico
Gulf of Mexico
Cuba
Western Sahara
Islamic Republic of Mauritania
Mali
Republic of Niger
Chad
Sudan
Nigeria
Burkina Faso
Guinea
Ghana
South Sudan
Ethiopia
Somalia
Kenya
Venezuela
Colombia
Ecuador
Brazil
Peru
Bolivia
Paraguay
Chile
Argentina
Uruguay
Gabon
DR Congo
Tanzania
Angola
Zambia
Mozambique
Namibia
Zimbabwe
Botswana
South Africa
Madagascar
Indian Ocean
South Atlantic Ocean
South Pacific Ocean
Indonesia
Banda Sea
Arafura Sea
Papua New Guinea
Coral Sea
Australia
Great Australian Bight
Tasman Sea
New Zealand

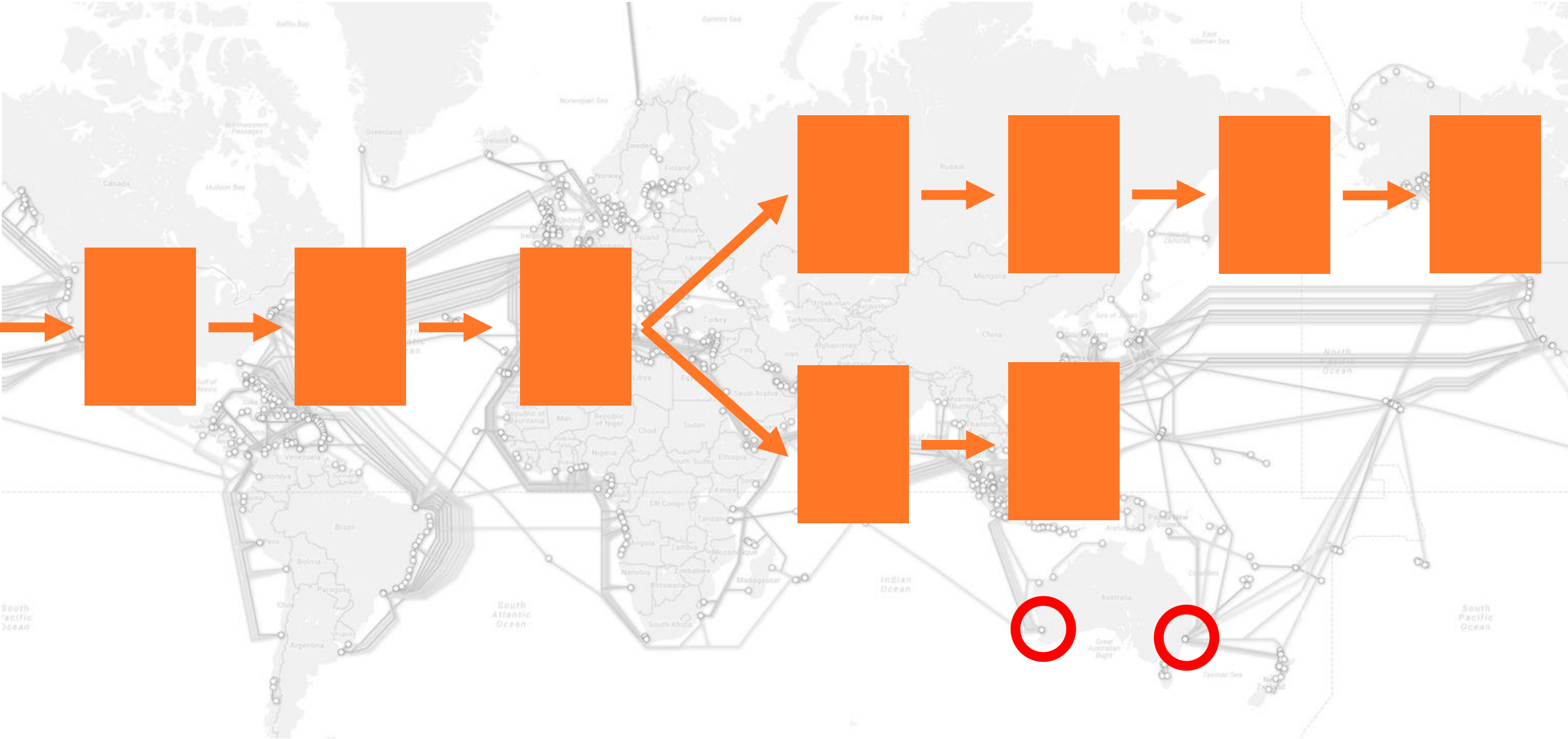


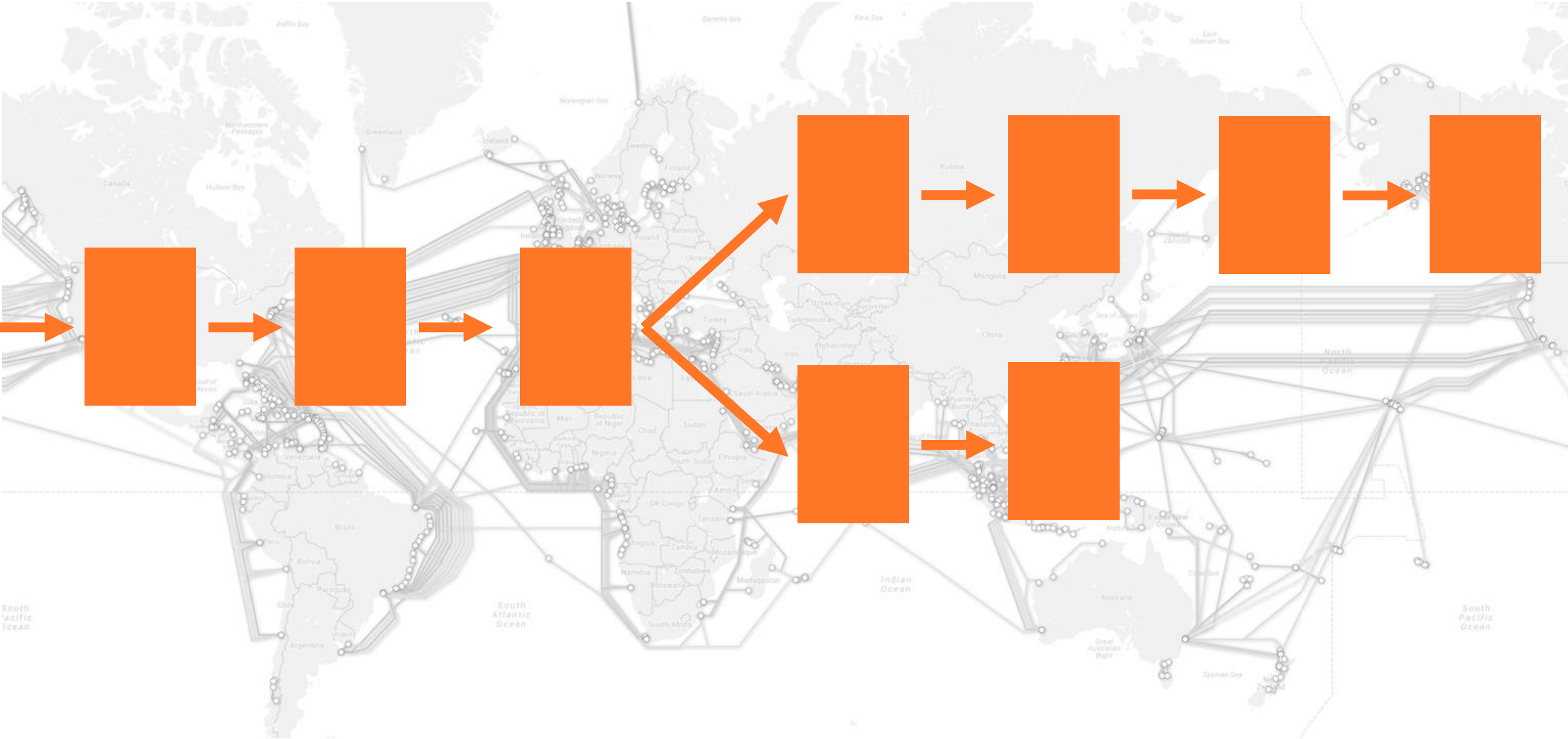


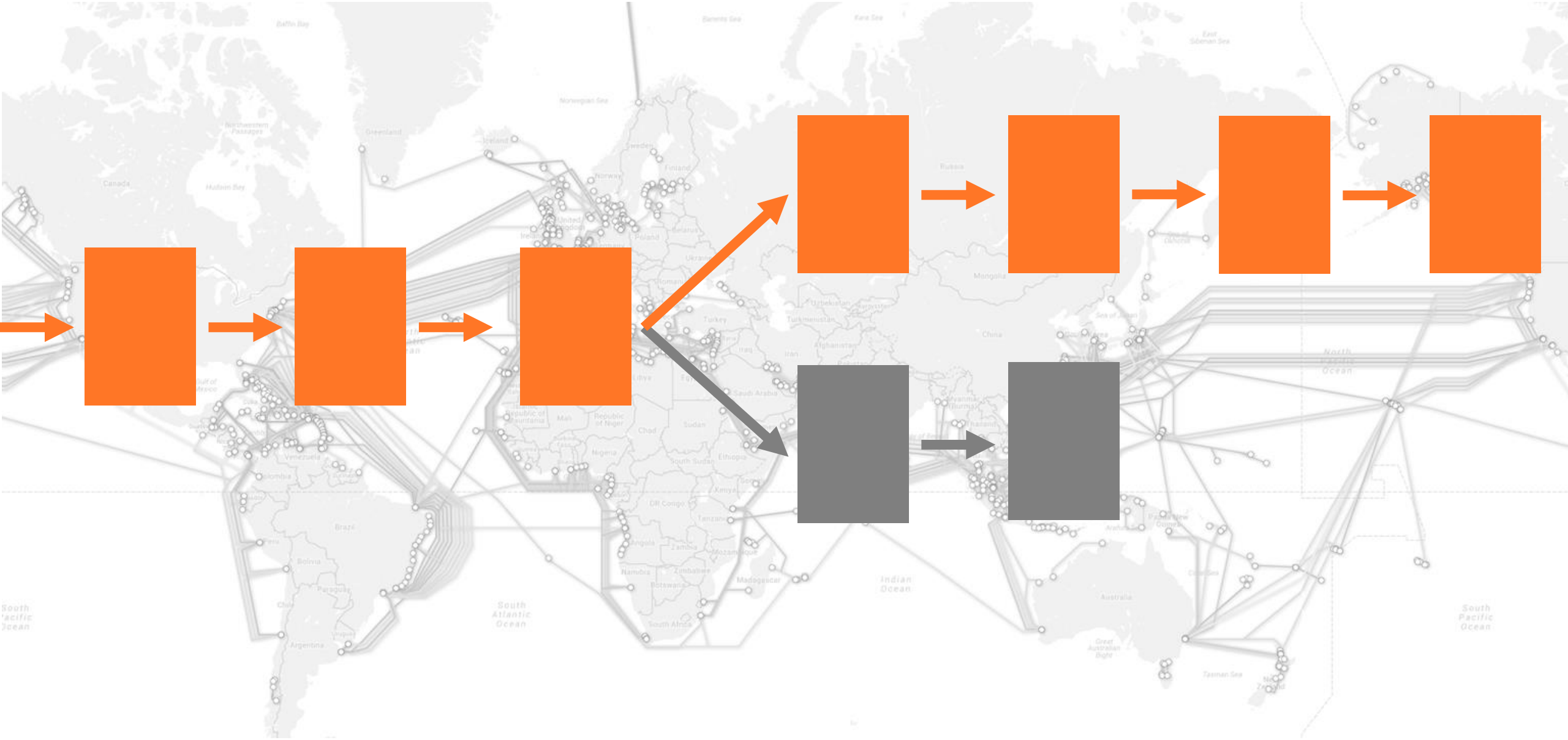


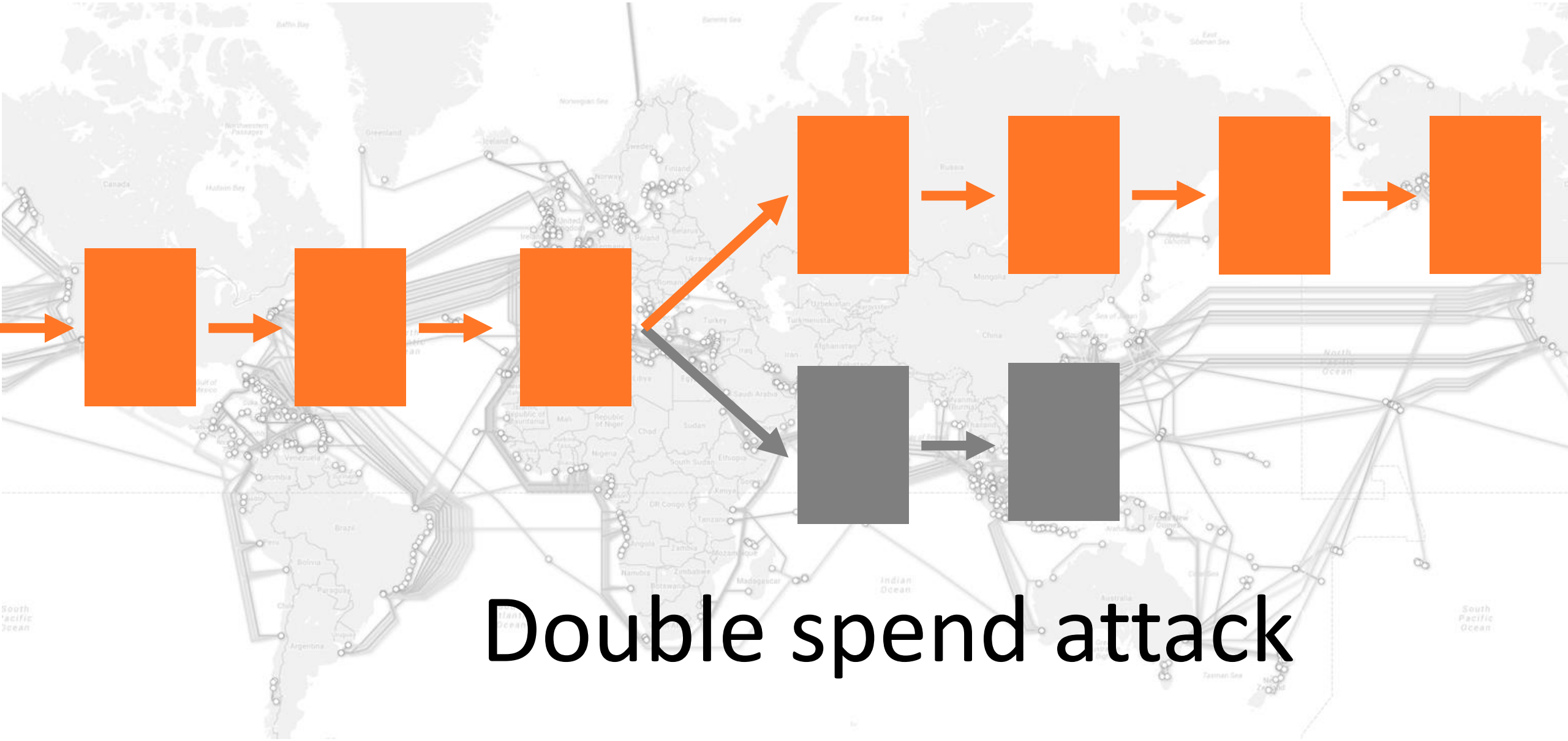












Double spend attack

Przepustowość sieci Bitcoin to około 5 transakcji na sekundę

Przepustowość sieci Bitcoin to około 5 transakcji na sekundę

… ale od 2019 roku w użyciu jest Lightning Network, który pozwala robić tymczasowe mini-blockchainy

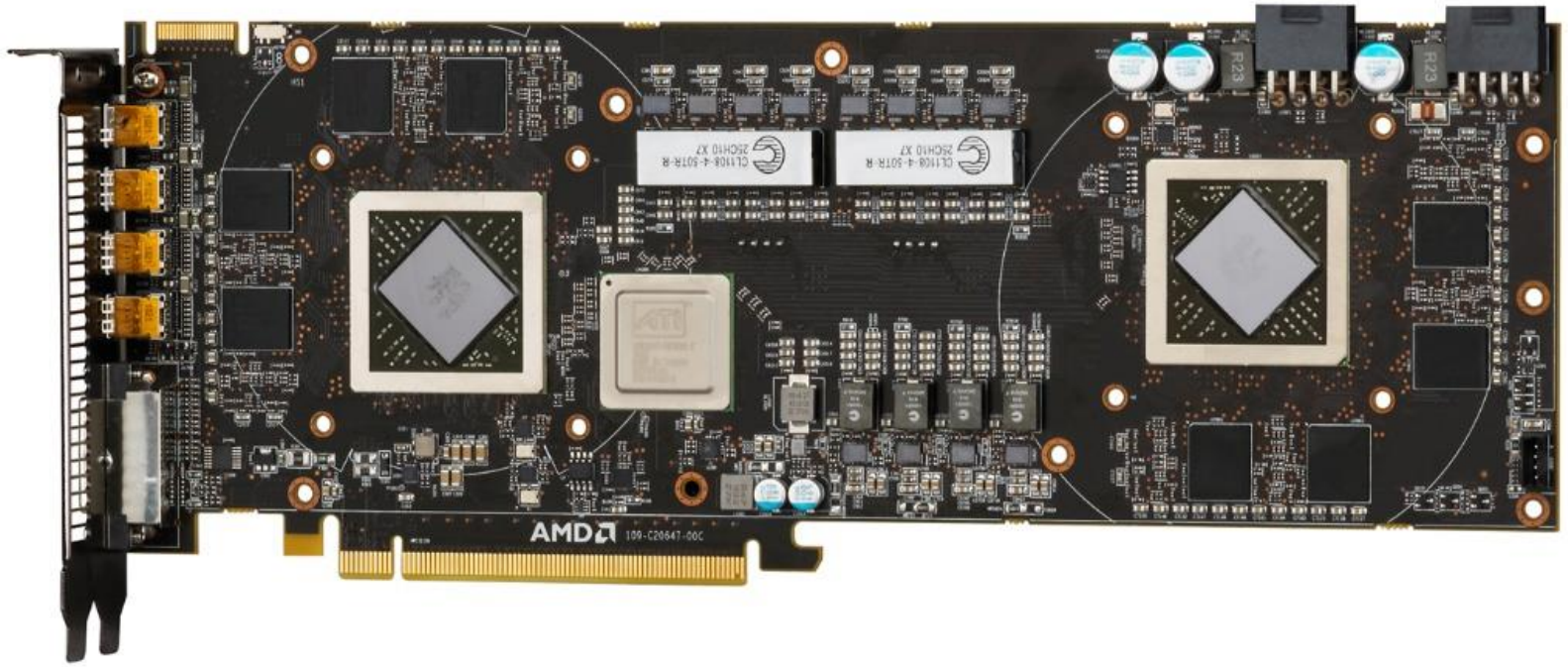
Co to jest kopalnia i czym się kopie bitcoiny

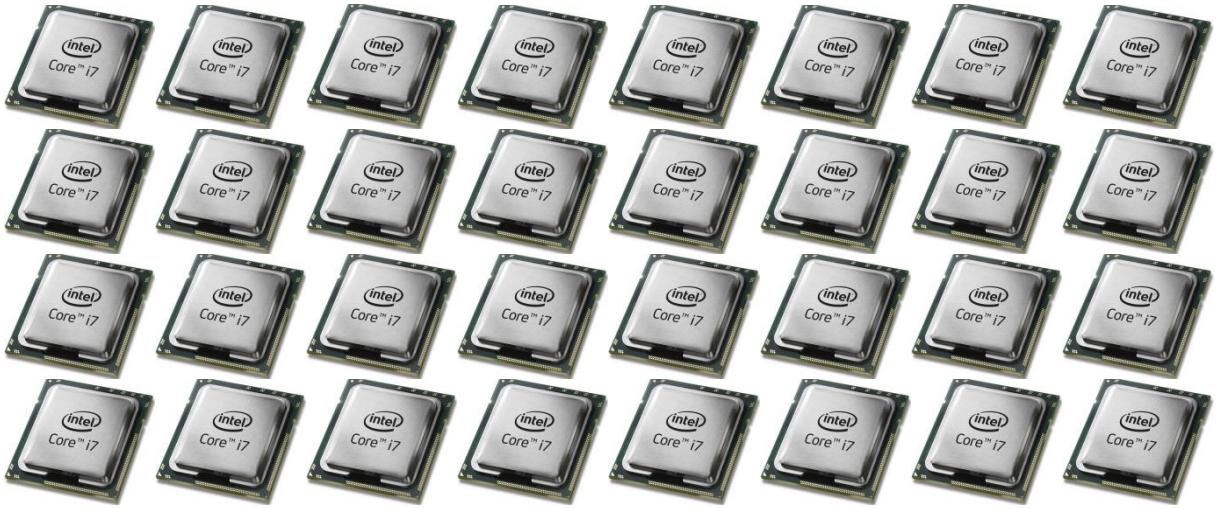
oraz Proof of Work

slido.com
#76766

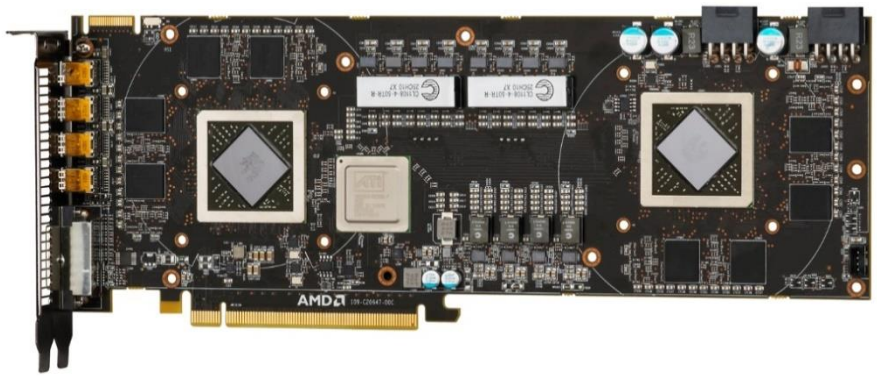
CPU Intel Core i7 2600 4c/8t
23.9 Mhps

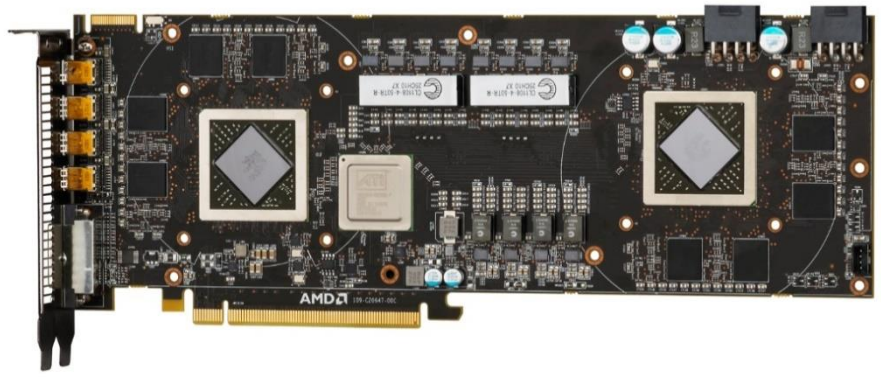
(23 900 000 hash/second)





Radeon 6990
800 Mhps





Radeon 6990 x3
2000 Mhps

Application-specific integrated circuit (ASIC)

Block Erupter

300 Mhps

49x ASIC Block Erupter

14700 Mhps

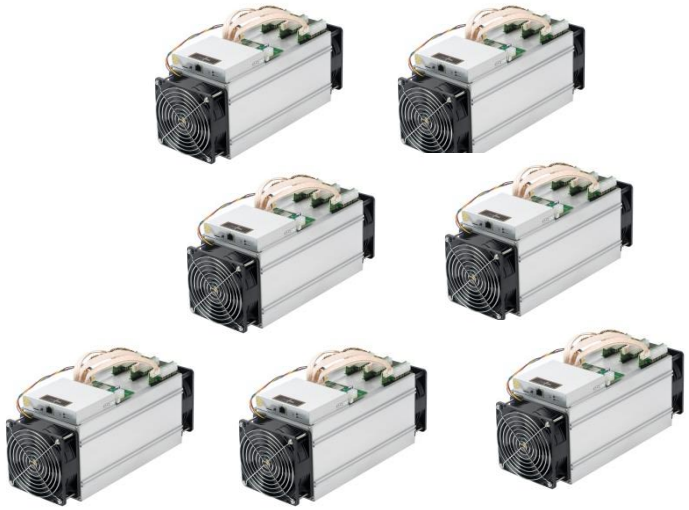
(14 Ghps)

Antminer T9

13500 Ghps (13,5 Thps)

Antminer T19

95 Thps
3300 W
$5000



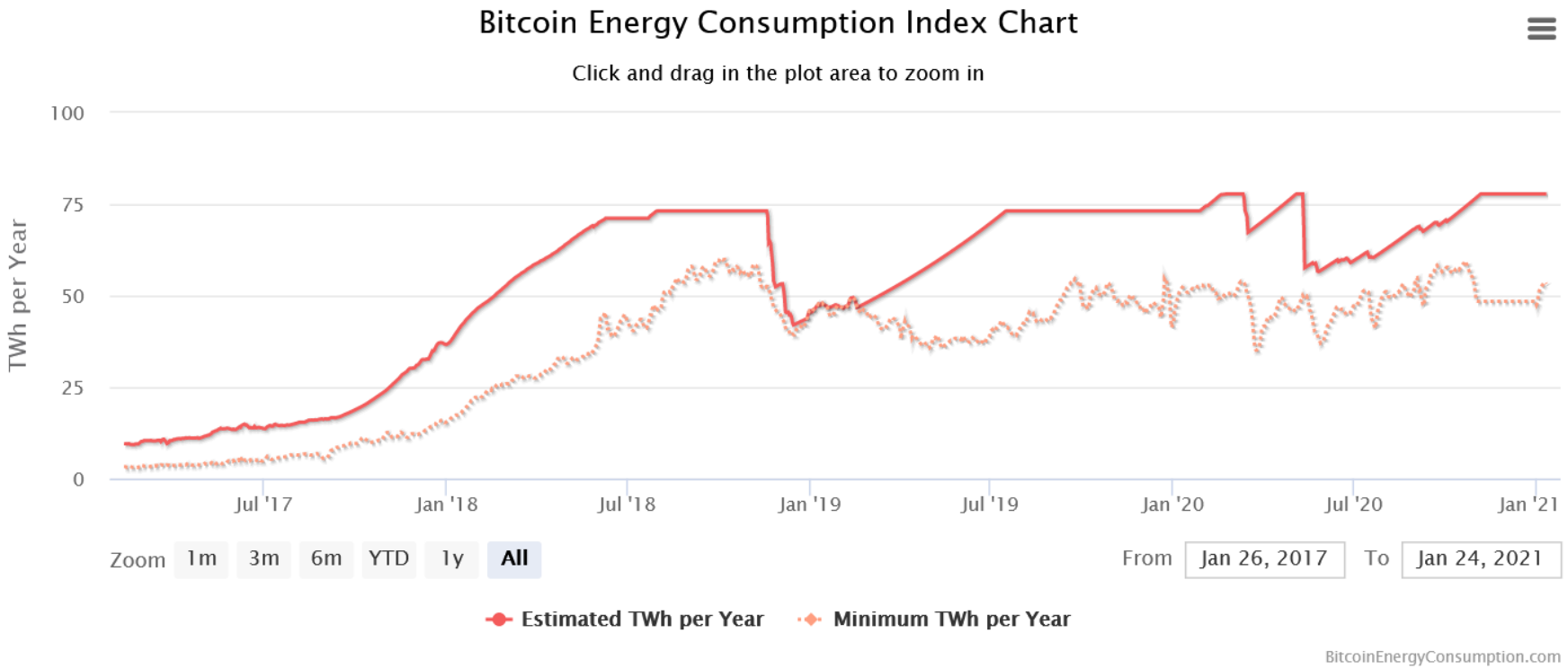
Kopalnia

«zakład górniczy zajmujący się wydobywaniem z ziemi kopalin»

«duże ilości naraz górników»

Spółdzielnia kopiących na wspólny rachunek i dzielących się zyskiem proporcjonalnie do włożonej mocy obliczeniowej.

Zużycie energii



633 kWh per transaction (~360 zł), **77 TWh rocznie**
Dla porównania: elektrownia Bełchatów – **28 TWh**

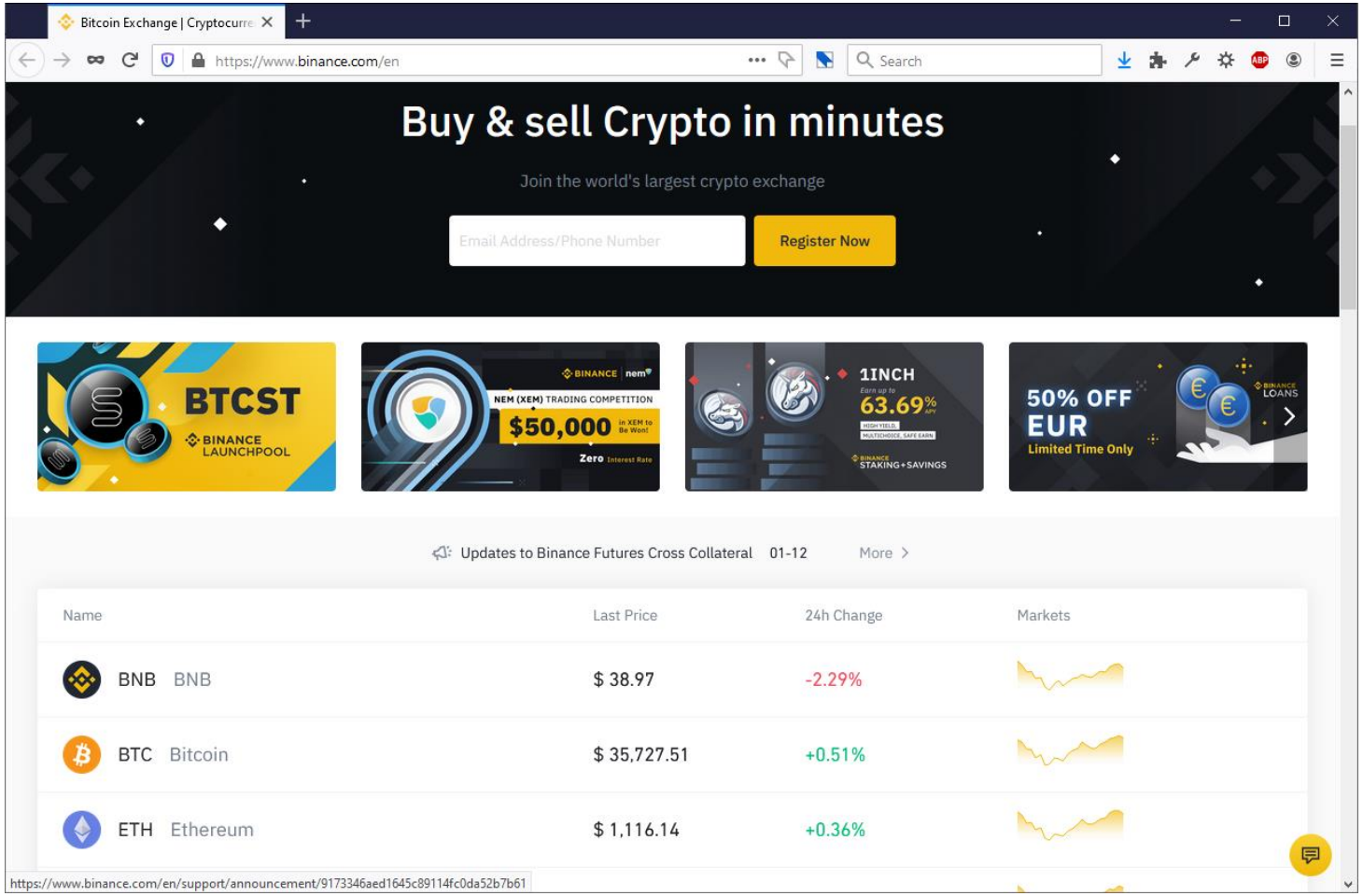
Jak przechowywać klucze prywatne

oraz jak je tracić

slido.com
#76766

W giełdzie kryptowalut

- Giełda może zostać shackowana i okradziona
- Właściciele mogą się oddalić w nieznanym kierunku



W oprogramowaniu na PC lub w telefonie

- Urządzenie możesz zgubić, zepsuć, spalić, wyrzucić lub utopić
- Backup też

- Masz w ogóle backup?

W portfelu papierowym

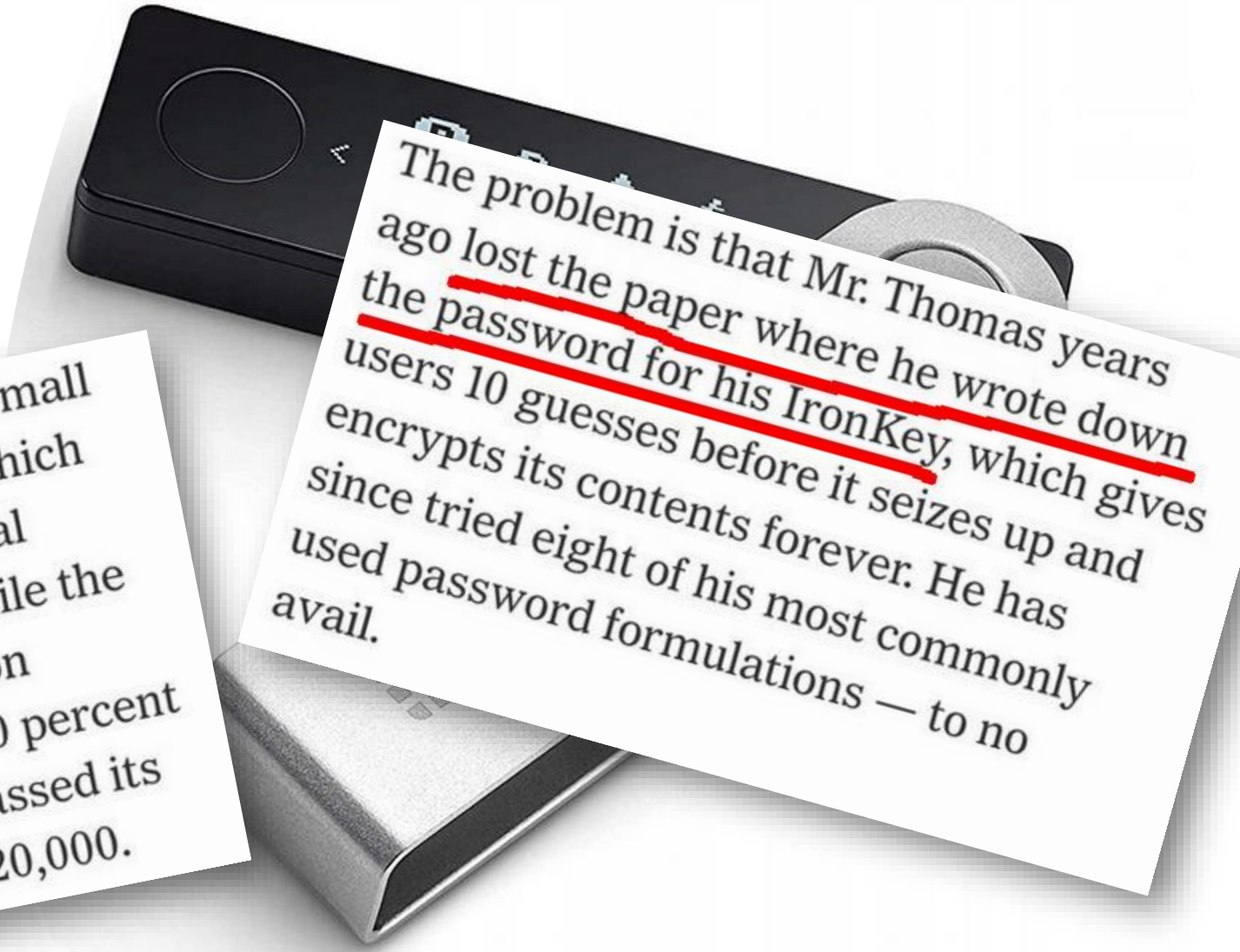
- Papierowy portfel możesz zgubić, zepsuć, spalić, wyrzucić lub utopić
- Unikalna cecha papierowego portfela – możesz pokpić sprawę wypłaty środków i utracić je na zawsze

W bezpiecznym urządzeniu

- Lista klientów może wyciec producentowi lub dystrybutorowi, dzięki czemu dostaniesz
  e-maile i telefony
  z groźbami, szantażem
  i próbą wymuszenia okupu

W bezpiecznym urządzeniu

- Lista klientów może wyciec
  producentowi l
  d
  d
  e-
  z g
  i pr



Do czego komu Bitcoin i kto to w ogóle wymyślił

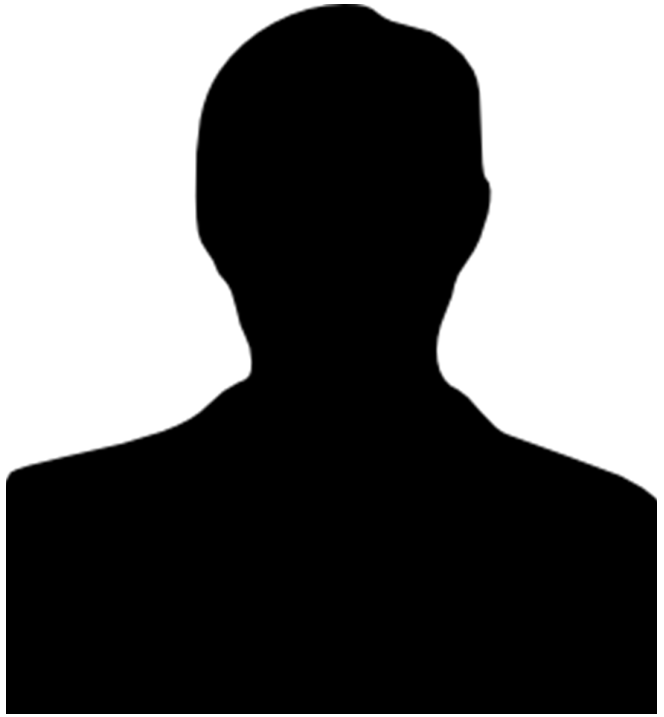
slido.com
#76766

Kto wymyślił Bitcoina

- Satoshi Nakamoto:
  - w 2008 zaprojektował protokół
  - w 2009 opublikował wzorcową implementację klienta sieci Bitcoin
- uważa się, że Satoshi w początkowym okresie działania sieci wykopał około miliona bitcoinów

Kto wymyślił Bitcoina

- Satoshi Nakamoto:
  - w 2008 zaprojektował protokół
  - w 2009 opublikował wzorcową implementację klienta sieci Bitcoin
- uważa się, że Satoshi w początkowym okresie działania sieci wykopał około miliona bitcoinów
- problem: nie wiadomo, kto kryje się pod tym pseudonimem
- Satoshi nie odezwał się od 2011



Zastosowania Bitcoina

- Opłacanie okupu za ransomware
- Zakup nielegalnych towarów i usług
- Inwestycja / spekulacja / HODL

(długo, długo nic)

- Zwykły obrót pieniężny (haha, nie)

Zastosowania blockchaina

- Generowanie marketingowego pierdolololo

(długo, długo nic)

- Nic

Dlaczego bitcoin jest wart XXXX dolarów?

Nie kupuj bitcoinów mając tylko wiedzę z tej prelekcji. Ucz się i ćwicz na małych kwotach!

INFORMATYK ZAKŁADOWY.PL