BLOCKCHAIN

Tomasz Śmiech; Rafał Kolaska

TOPOLOGIA SIECI

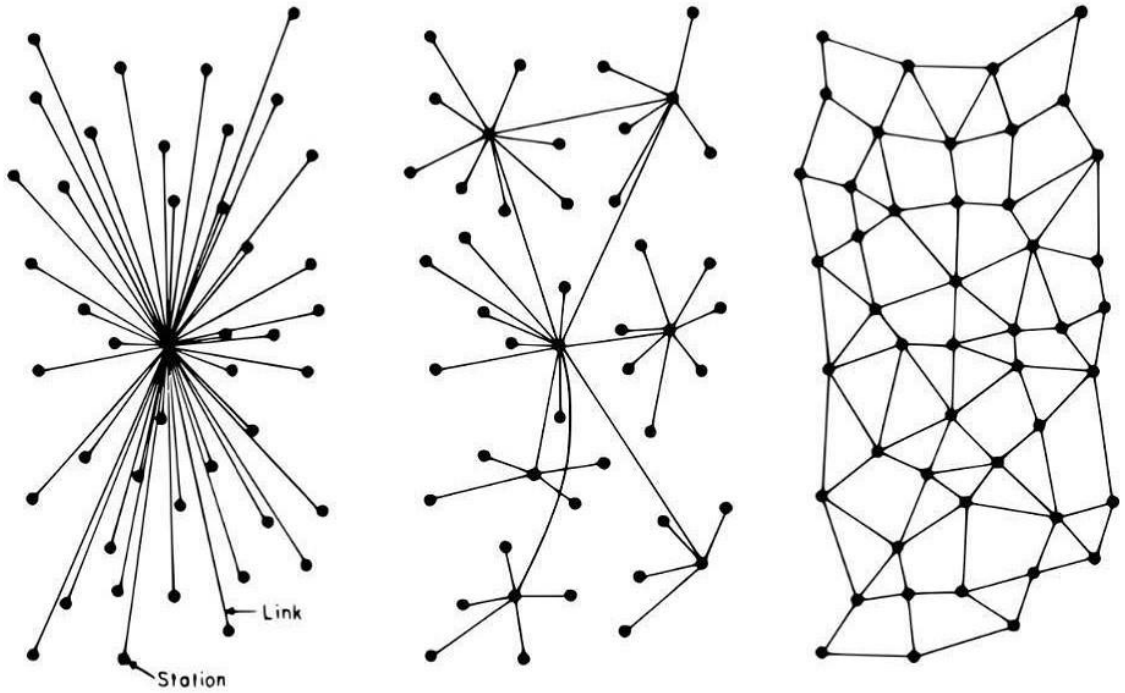


FIG. 1 — Centralized, Decentralized and Distributed Networks

P2P (Peer-to-peer)

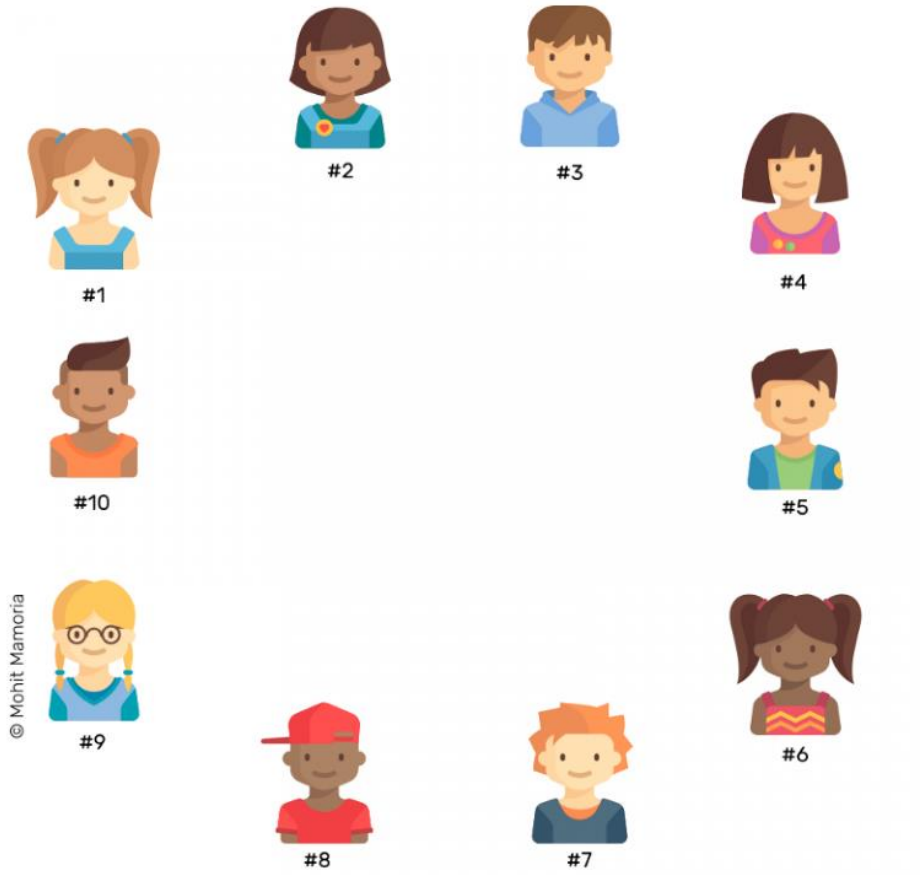
Model komunikacji w sieci komputerowej, w którym każdy host ma te same uprawnienia, każdy może jednocześnie pełnić role klienta i serwera. Zaletą tego typu modelu jest brak centralnego serwera.

Łańcuch bloków

*“**Blockchain** – zdecentralizowana i rozproszona baza danych w modelu open source w sieci internetowej o architekturze peer-to-peer (P2P) bez centralnych komputerów i niemająca scentralizowanego miejsca przechowywania danych, służąca do księgowania poszczególnych transakcji, płatności lub zapisów księgowych zakodowana za pomocą algorytmów kryptograficznych.”*

-Wikipedia

Jak działa sieć?



Osoba numer 1 przesyła 10 BTC do osoby numer 5.
Akcja zostaje zanotowana na liście.

11.03.2019	Nr 1	Nr 2	10 BTC

Po pewnej ilości transakcji lista zostaje zapełniona

11.03.2019	Nr 1	Nr 2	10 BTC
11.03.2019	Nr 5	Nr 7	1 BTC
12.03.2019	Nr 1	Nr 10	2 BTC
14.03.2019	Nr 4	Nr 2	5 BTC

Rozpoczyna się szyfrowanie

Szyfrowanie

Do szyfrowania informacji wykorzystywany jest algorytm SHA-256

“Ala ma kota” →  → 001231abcda

“ala ma kota” →  → 01446abcdaw

Algorytm jest czuły na zmiany danych wejściowych
Posiadając szyfr nie jesteśmy w stanie ustalić danych wejściowych

Szyfrowanie

Skomplikujmy problem :

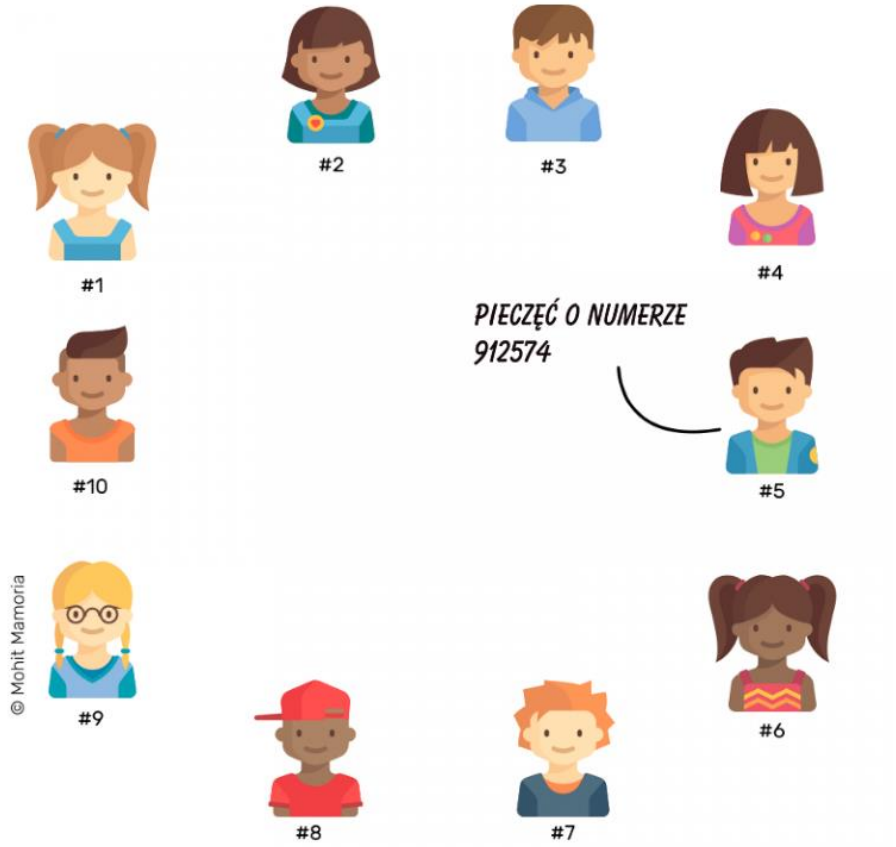
Lista transakcji + ?

0000…

Lista transakcji
+
912574

0000abttr2

Szyfrowanie



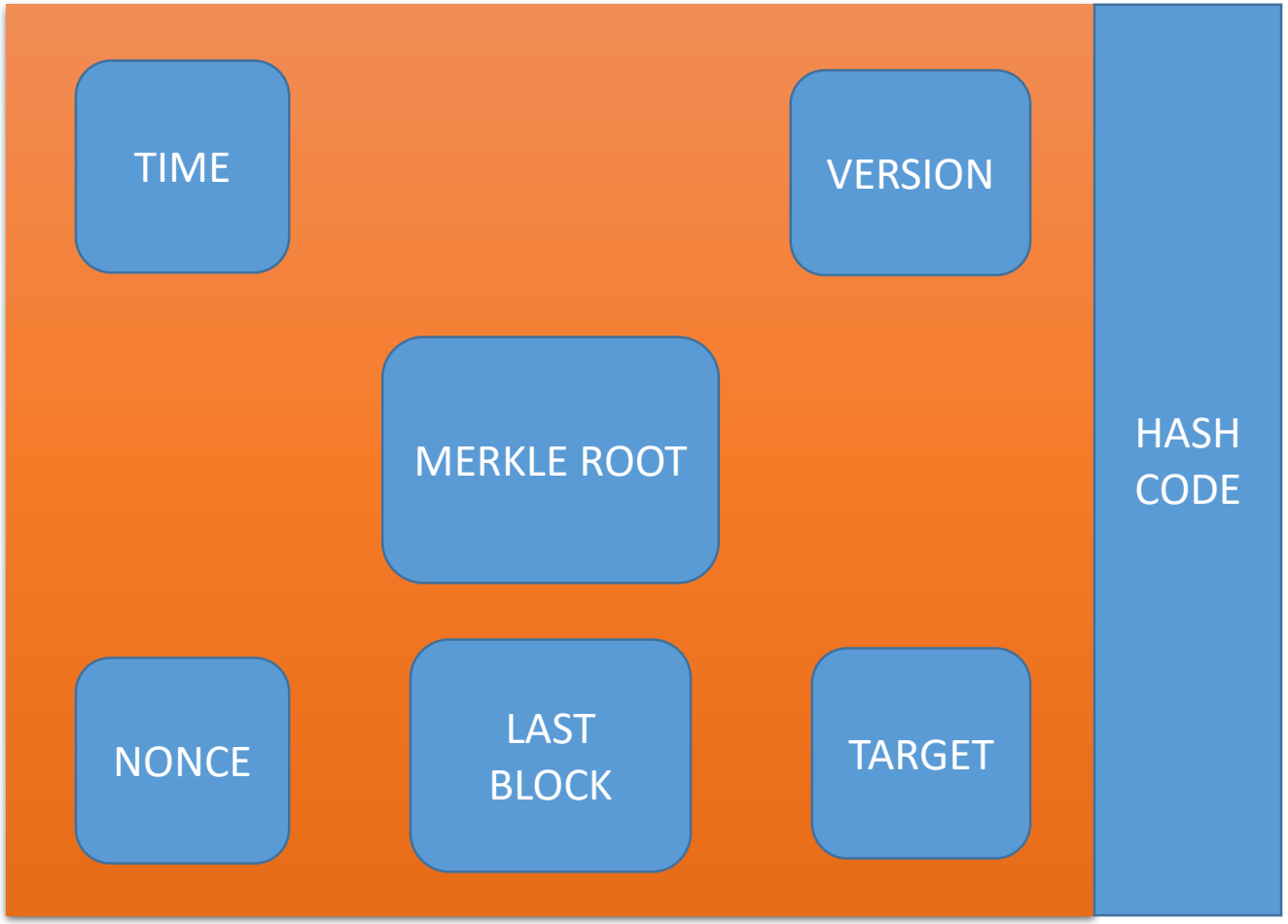
Po zapisaniu listy każdy z uczestników sieci rozpoczyna szyfrowanie.

Wynik:

912574
Proof of Work

Następuje kontrola przez resztę członków.

Struktura Bloku



Cechy technologii Blockchain

1. **Decentralizacja**
2. **Transparentność**
3. **Niezmienniczość**

Decentralizacja

W sieci tej brakuje centralnego serwera gdzie składowane byłyby dane, a przekazywanie między sobą informacji przebiega bez pośredników.

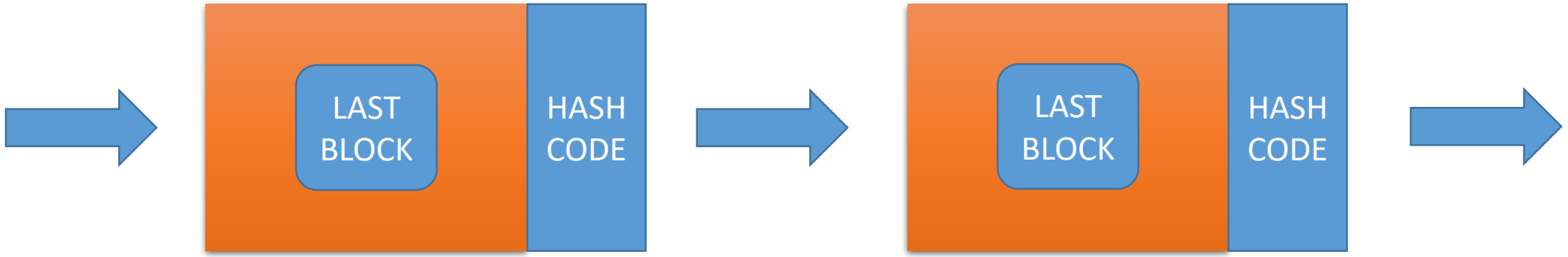
Transparentność

Wszystkie akcje przeprowadzane w sieci są widoczne dla każdego użytkownika, jednak on sam pozostaje anonimowy. Identyfikowany jest jedynie za pomocą publicznego adresu.

TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...		0x2bdc9191de5c1b...	0.004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...		0xf14cb3acac7b230...	0.744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...		0x2d42ee86390c59...	0.016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...		0xd39681bb0586fb...	0.01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...		0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...		0x8a91cac422e55e...	0.029594 Ether	0.000294

Niezmienniczość

Dzięki własności funkcji szfrującej oraz budowy bloku dane są nie do zfałszowania.



System przechowywania plików

- składowanie w aplikacji blockchain,

- system plików p2p,

- zdecentralizowana chmura,

- rozproszona baza danych,

- BigChainDB,

- TiesDB,

Zastosowanie

- rejestr do zarządzania aktami własności i nieruchomości (Gruzja),
- połączenie publicznych baz danych (Estonia),
- wprowadzenie wirtualnych walut narodowych (Singapur),
- system do obsługi polis ubezpieczeniowych (IBM, USA, Kenia),
- przeglądarka internetowa BRAVE,

https://www.quora.com/How-can-blockchain-be-used-as-a-database-to-store-data

https://blog.kurasinski.com/2017/07/czym-jest-do-cholery-blockchain/

https://blockgeeks.com/guides/what-is-blockchain-technology/

https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf/77392774-1180-79ab-4dd5-089ffab37602

http://learnmeabitcoin.com/guide/blocks

http://insurancemarketresearch.com/global-peer-to-peer-fundraising-software-market/

https://pl.wikipedia.org/wiki/Blockchain

https://bithub.pl/felietony/technologia-blockchain-wykorzystanie/

P. Baran, *On Distributed Communication Networks*