Rafał prostuje Blockchain: Blockchain jako baza danych i dlaczego adresy nie istnieją

Poznań, FlyingAtom, 17. lutego 2018

Łańcuch ~~bloków~~ slajdów

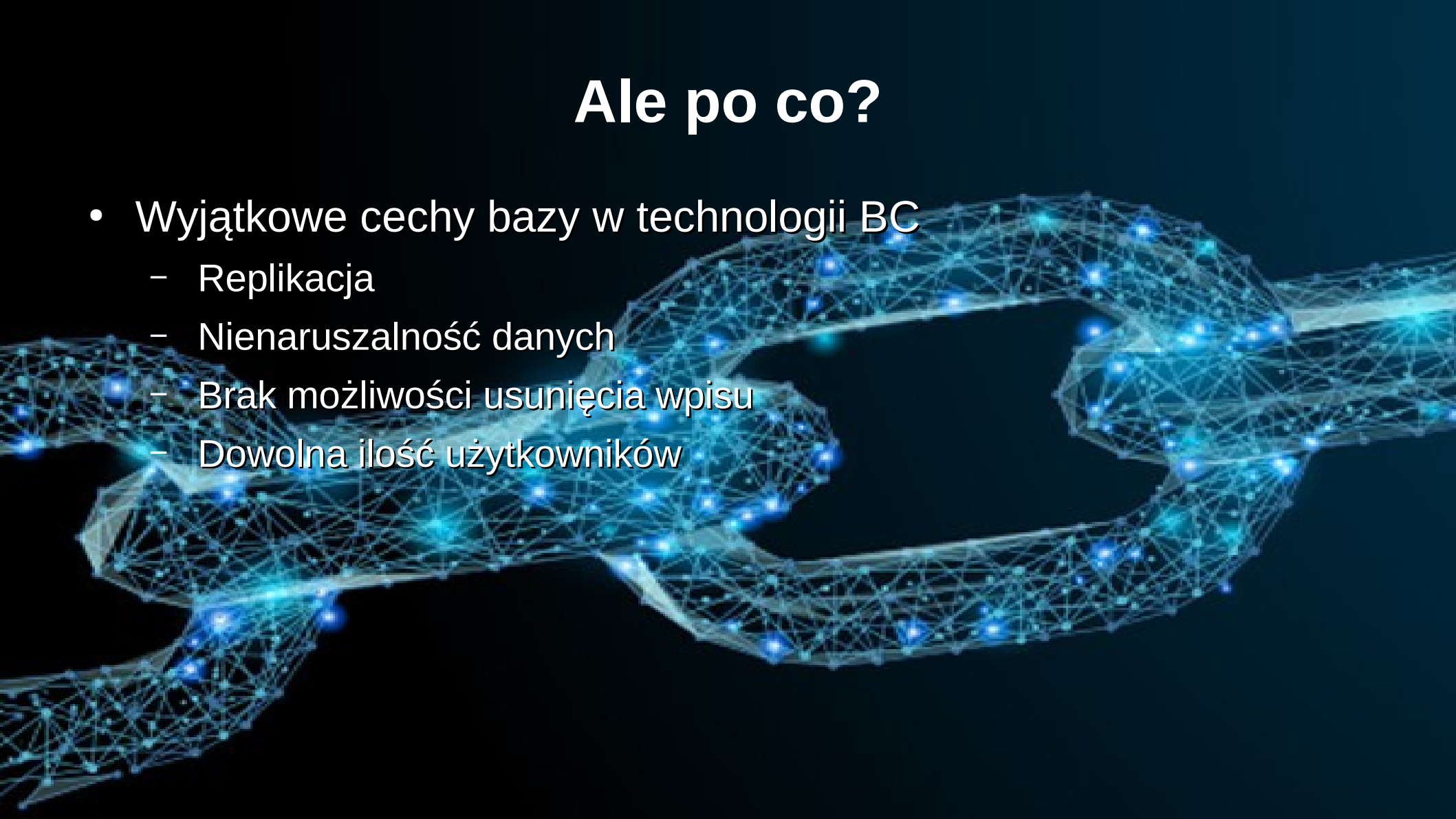
- Blok 0/genesis
  - Co zawiera blockchain
  - Czego nie powinien zawierać
  - A po co nam taka słaba baza danych
- Blok 1/premine
  - O transakcji słów kilka
  - Na początku było wyjście
  - Baza UTXO
  - Wydajemy wejścia
  - Kto to ten Schnorr?

Blockchain = baza danych

- Zawartość BC
  - Bloki transakcji
- Czego nie warto trzymać
  - Dużej ilości danych

Ale po co?

- Wyjątkowe cechy bazy w technologii BC
  - Replikacja
  - Nienaruszalność danych
  - Brak możliwości usunięcia wpisu
  - Dowolna ilość użytkowników



Budowa transakcji

- Transakcja jako zapis księgowy
  - Kto
  - Komu
  - Ile
- Transakcja jako zapis do bazy
  - Kto
  - Co

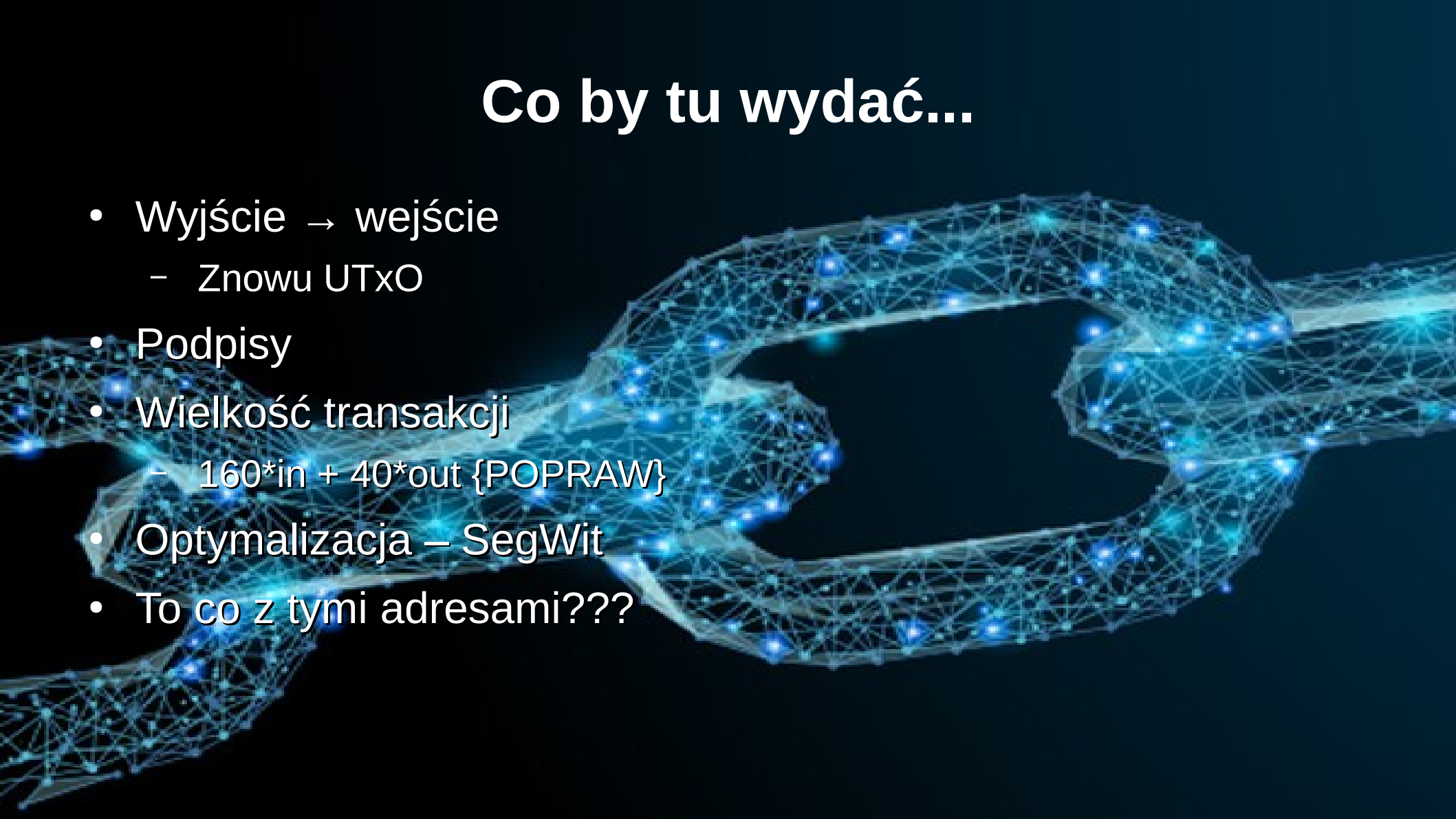
Kura czy jajko?

- Zwykła transakcja
  - Kto → komu
- Transakcja generacji
  - Sieć → komu

Baza UTxO

- Unspent Transacion Outputs
- Co było przed UTxO
- Obecne użycie
- Co ma do tego pruning

Co by tu wydać...



- Wyjście → wejście
  - Znowu UTxO
- Podpisy
- Wielkość transakcji
  - 160*in + 40*out {POPRAW}
- Optymalizacja – SegWit
- To co z tymi adresami???

Pan Schnorr

- KRYPTOVOOOODOOOO
- Łączenie podpisów
  - Jeden podpis dla wielu wejść
  - Jeden podpis na transakcję

Kwestions & Ansfers

- ?
- ??
- ???
- Sprzedane!

Dziękuję! :)