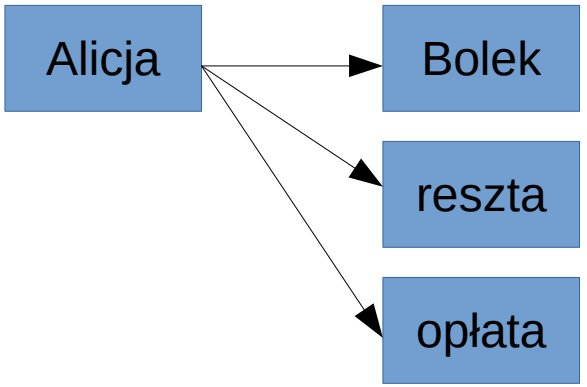
Transakcje 007

Czyli transakcje do zadań specjalnych

Budowa typowej transakcji P2KH

Wejście → wyjście



Wejście1 = UTXO[TXID+nr] ←(Alicja)
Wejście2 = UTXO[TXID+nr] ←(Alicja)
...
Wyjście1 = adres odbiorcy → (Bolek)
Wyjście2 = adres reszty →(Alicja)
...
Opłata = we-(wy1+wy2) → (górnik)

Bilans transakcji = zawsze 0

- Moje wyjście = czyjeś wejście
- Opłata transakcyjna (tx fee)
- Podwójne wydanie (double spend)

Baza transakcji

- Powiązania transakcji
  - Unikalność hasza transakcji – „transaction mallebility”
  - Kolejność (łańcuch) transakcji
- UTXO - Unspent Transaction Output (niewydane wyjście z transakcji)
  - Z czego budować?
  - Jak używać?
  - (Bitcoin Core) portfel, UTXO i txindex
- Problemy
  - Przesyłanie (WIP)

Blok czyli paczka (danych)

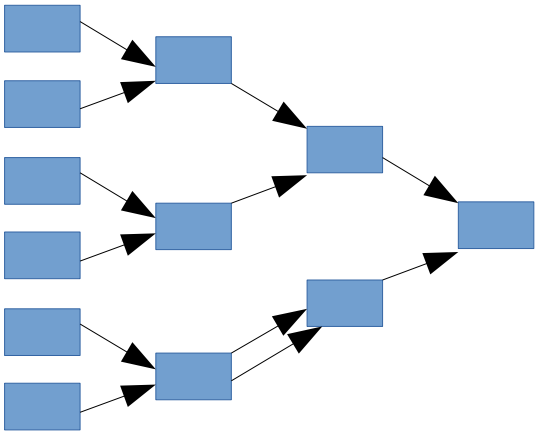
Budowa bloku

Kod [4]	rozmiar[4]	nagłówek[80]	Licznik[1-9]	transakcje

Nagłówek

wersja	hasz poprzedniego bloku	hasz drzewa [MTH]	czas	trudność	licznik

- Transakcja generacji (Coinbase) – brak wejścia
- hasz drzewa haszy transakcji - Merkle Tree Hash Root



Bezpieczeństwo bloków

- Łańcuch bloków - wysokość/długość/głębokość
- Proof of Work
- Forkowanie
  - Przy kopaniu
  - Na miękko
  - Na twardo

Zapisy w blockchainie

- Tekst w transakcji generacji (coinbase)
  - Blok „0” (zero)
  - Głosowanie P2SH
  - Obecne użycie
- Adresy
  - Proof of burn
  - Zagrożenie dla bazy UTXO
- Nowość! OP_RETURN [80]

Istniejące zapisy

- Manifest w PDF (blok 230009)
- Logo bitcoin.png (yEnc)
- ASCII-art
- Atak XSS
- Zdjęcia
- Wikileaks „cablegate” 2.5MB 7z
- Walentynki
- ...