Ewolucja giełd zdecentralizowanych

Jacek Wytrębowicz

Instytut Informatyki Politechniki Warszawskiej

Co chciałbym przedstawić?

- Okresy rozwoju giełd
- Specyficzne dla giełd aspekty bezpieczeństwa
- Kierunki rozwoju
- Giełdy w liczbach
- Co z tego wynika?

Rys. złożony przez: ChatGPT/

Okresy rozwoju giełd

1. Rozwiązania scentralizowane – 2010-2015
2. Wczesne rozwiązania zdecentralizowane – 2015-2017
3. Klasyczne DEX-y – 2016-2020
4. Obudowa DEX-ów – 2020-2022
5. RFQ i rozkwit DEX-ów – 2021-2024
6. Rozwój CEX, DEX i hybrydowych – 2023-…

2010-2015 – rozwiązania scentralizowane

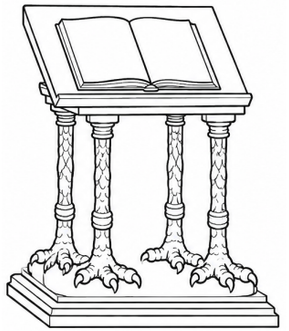
- ✦ Dominacja scentralizowanych ksiąg zleceń (np. Mt. Gox)
  - szybkie przetwarzanie
  - wysoka płynność

- ✦ Scentralizowane platformy komunikacyjne peer-to-peer (np. LocalBitcoins)
  - nawiązywanie kontaktu
  - wspomaganie wymiany

Platformy scentralizowane rozwijane są do dziś!

2015-2017 – wczesne rozwiązania zdecentralizowane

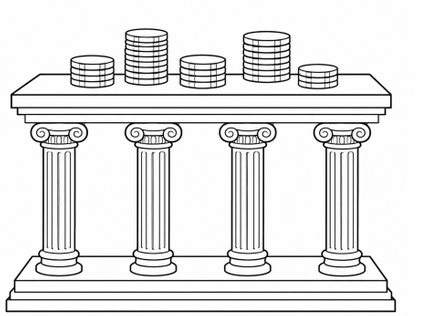
- ✦ Zdecentralizowane księgi zleceń (np. EtherDelta i IDEX)
  - okazały się nieskalowalne



- ✦ Zdecentralizowane platformy komunikacyjne peer-to-peer (np. Bitsquare → Bisq)
  - przenoszą oferty
  - wolne transakcje
  - mała płynność
  - wysokie spready

2016-2020 – klasyczne DEX-y

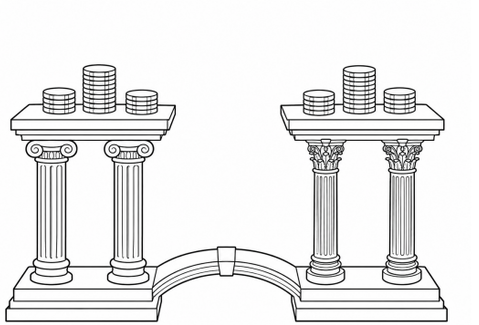
- ✦ Rozpowszechnienie się AMM, ang. Automated Market Maker, (np. Bancor «2017», Uniswap v1)
  - ciągła płynność
  - uboga funkcjonalność
  - nieprzyjazne interfejsy
  - efektywne dla wymian o małej wartości
  - działają na jednym blockchainie (najwięcej na Ethereum)



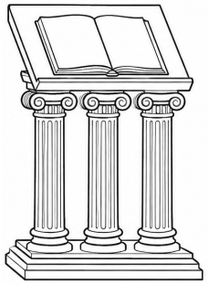
- ✦ Giełdy NFT (np. OpenSea, Synthetix «Havven 2018», dYdX, Perpetual Protocol)

2020-2022 – obudowa DEX-ów

- Agregatory DEX (np. 1inch)
  - używają platform mostów międzyblockchainowych

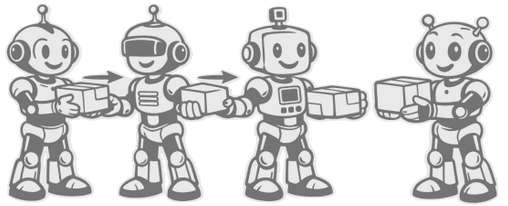


- Rozwiązania hybrydowe – księga zleceń off-chain a wymiana on-chain (np. IDEX, dYdX v3)
  - szybkie przetwarzanie
  - większe bezpieczeństwo
  - możliwe procesy KYC i AML



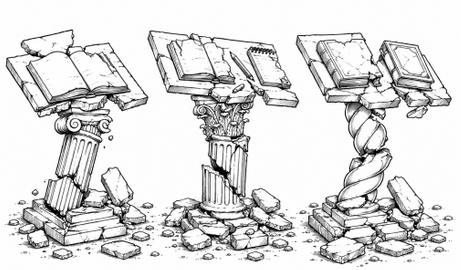
2021-2024 – RFQ i rozkwit DEX-ów

- ✦ Protokoły RFQ, ang. Request For Quote, (np. 0x RFQ, UniswapX)
  - przetwarzanie ofert off-chain, wymiana on-chain
  - przenoszę zobowiązania, działają algorytmicznie
  - wysoka płynność
  - obsługa transakcji hurtowych w odróżnieniu od komunikatorów P2P

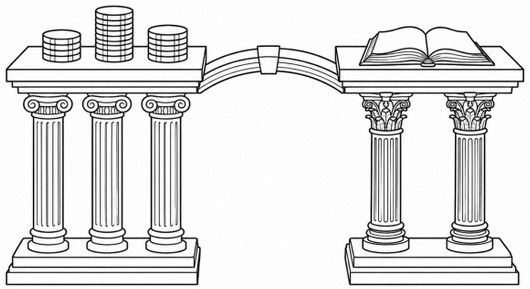


2022 – bankructwa scentralizowanych platform DeFi

FTX, Terra-Luna, Celsius, Three Arrows Capital, Voyager Digital, BlockFi…

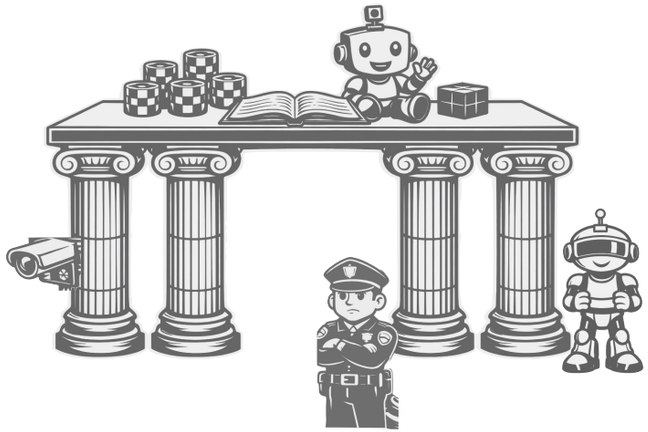


- ✦ Zaawansowane rozwiązania hybrydowe (np. Osmosis)
  - przyjazne interfejsy
  - bogate funkcjonalnie frontendy
  - interoperacyjność – integracja mostów kryptograficznie weryfikowalnych



2023-… – rozwój CEX, DEX i hybrydowych

- ✦ Dodatkowe przetwarzania w warstwie wykonawczej on-chain i off-choin
  - hybrydy AMM, księgi zleceń i RFQ
  - obsługa zleceń intencjonalnych (np. CowSwap)
  - powstrzymywanie ataków MEV, ang. Maximal Extractable Value
  - programowalne AMM – wtyczki



Aspekty bezpieczeństwa

- ✦ Przeciwdziałanie nadużyciom MEV (ang. Maximal Extractable Value) – od 2021
  - szyfrowanie transakcji
  - dowody z wiedzą zerową, ang. zero-knowledge proof
  - mechanizmy powstrzymywania w warstwie wykonawczej giełdy
    - prywatne pule transakcji
    - losowe porządkowanie transakcji
    - blokowanie wartości uzyskanej w transakcji zidentyfikowanej jako MEV

- ✦ Wykrywanie handlu pozornego, ang. wash trade – od 2021
  - rejestrowanie użytkowników i wdrażanie algorytmów wykrywających

- ✦ Dowody przechowywanych rezerw – od 2021
  - mechanizmy dowodów z wiedzą zerową zk-SNARK i zk-STARK (np. Loopring)

- ✦ Anonimowość i poufności transakcji – od 2022
  - szyfrowanie zleceń (np. Renegade)
    - dowody z wiedzą zerową i wielostronne obliczenia prywatne, ang. Multi-Party Computation

- ✦ Kontrola ryzyka – od 2023
  - cele:
    - ograniczanie strat systemowych
    - zapewnienie płynności
    - utrzymanie stabilności
  - mechanizmy (smart kontrakty):
    - bezpieczniki rynkowe, ang. circuit breakers
    - analizatory zleceń

- ✦ Zgodność z regulacjami AML – od 2023 frontendy DEX-ów
  - rejestracje zachowujące prywatność
  - listy obserwacyjne – adresy o podwyższonym ryzyku
  - ograniczenia geograficzne (np. dYdX v4)
  - usługi firm analitycznych (np. Chainalysis, TRM Labs, Elliptic)

Kierunki rozwoju

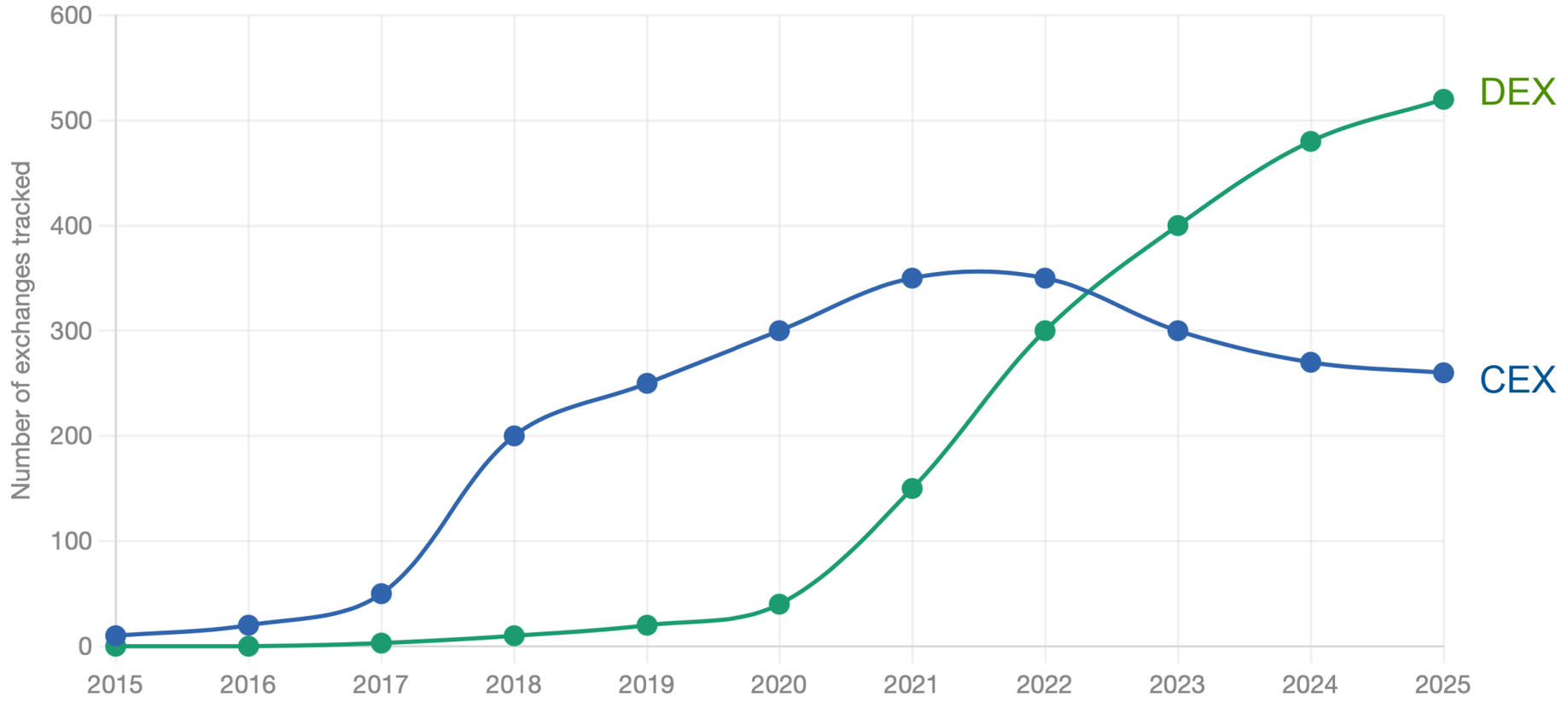
- ✦ Programowlność architektur giełdowych
  - konfigurowalne AMM-y, np. Uniswap v4 może uruchamiać wtyczki przed lub po
    - inicjalizacji puli tokenów
    - dodawaniu lub usunięciu tokenów z puli
    - wymianie tokenów
    - zbieraniu opłat za wymianę
  - portfele abstrakcji kont – od 2023
    - dowolne mechanizmy podpisu (np. WebAuthn, biometria)
    - łączenie wielu operacji w jedną transakcję
    - sponsorowanie płatności za transakcje
    - płacenie za gaz wybranymi tokenami (np. stablecoinami)…
- ✦ Infrastruktury programistyczne dla interoperacyjności
  - DEX jako komponent dla złożonej DApp (np. 0x, Loopring Protocol)
- ✦ Appchainy (np. dYdX v4)
  - natywne moduły węzłów zamiast smart kontraktów
- ✦ DEX-y w warstwach drugiej i trzeciej blockchainów

Giełdy w liczbach

Szacunek średniej liczby giełd w rankingach – CEX vs DEX

	#CEX	#DEX	w dniu
Forbes.pl [1]	> 300	> 140	23.12.2021
CoinMarketCap	> 240	> 300	16.02.2023
CoinMarketCap	257	389	12.12.2025
CoinMarketCap	240	385	2.06.2026
CoinGecko	177	1 165	2.06.2026
DeFiLlama	78	729 (138 agr.)	2.06.2026
Messari	174	124	2.06.2026

1/ https://www.forbes.pl/forbeswomen/inwestycje-w-kryptowaluty-gieldy-kryptowalut-dla-poczatkujacych-graczy/57542rr



Notes on methodology: CEX counts reflect exchanges tracked by CoinMarketCap/CoinGecko spot rankings (actively reporting volume). DEX counts reflect protocols tracked by DefiLlama and CoinGecko DEX rankings. Pre-2020 DEX figures and pre-2017 CEX figures are estimated from historical sources. "Tracked" ≠ "active" — many listed exchanges have minimal volume. CEX count decline after 2021 reflects delistings, collapses (FTX etc.), and tighter data-quality filters by trackers, not necessarily fewer real platforms

Źródło: https://claude.ai

Źródło: https://messari.io/exchanges

Szacunek liczby rodzai giełd zdecentralizowanych

Rodzaj giełdy	Szacowana liczba	Udział w rynku
AMM	setki – tysiące	~80 – 85%
Order Book	dziesiątki	~10 – 12%
RFQ	~10 – 20 godnych uwagi	~3 – 5%
Aggregators	~20 – 30 godnych uwagi	

Źródło: https://claude.ai

Podsumowanie

Współistnienie różnych

- CEX-ów, DEX-ów i hybryd
- księg zleceń i AMM
- komunikatorów P2P dla ofert i zobowiązań
- agregatorów

Rozwój

- SDK
- mostów międzyblockchainowych
- platform usługowych dla DeFi
  - analityka
  - bezpieczeństwo
- DeFi z usługą wymiany

Dążenie do poprawienia:

- interoperacyjności (tj. współpracy z wieloma blockchainami)
- funkcjonalności
  - łączenie zdecentralizowanych i scentralizowanych usług
  - dbałość o satysfakcję użytkownika
- efektywności – realizowanie szybszych i tańszych transakcji
- elastyczności – programowalność