FuturesMEX
Secure, Distributed Futures Market Exchange

Fabio Massacci[1], **Nam Ngo**[1], Jing Nie[2], Daniele Venturi[3], Julian Williams[4]
[1]**University of Trento, Italy**, [2]University of International Business and Economics Beijing, China
[3]University of Rome, Italy, [4]Durham Business School

Nowadays, all Futures Market Exchanges are centralized

A futures market is a double auction market with multiple bidders from both buy and sell side.
The participants are called traders and they bid and ask for futures contracts which are standardized promises made today and to be fulfilled in a future date.

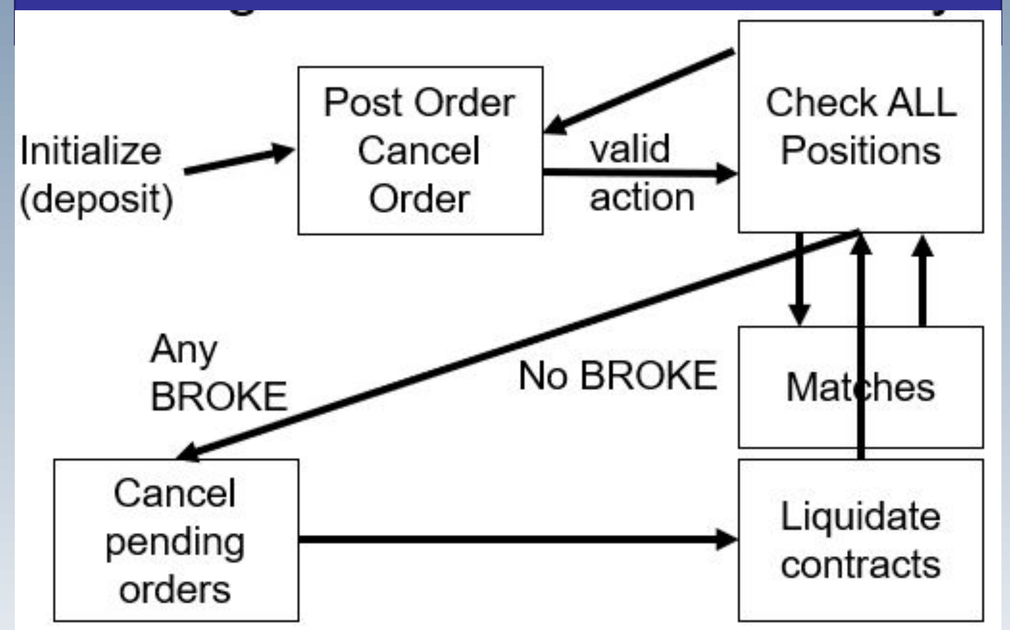
Purposes of an Exchange

Publish the order book
- Aggregate all orders
- Protect traders anonymity

Match orders

Manage risks
- Price oscillates
- High frequency traders (HFTs)

Exchange Functionality



ALL Technical Challenges MUST BE SOLVED AS ONE

Easy to see
- Market integrity
- Consensus

Less obvious
- Account confidentiality
- Trader anonymity
- Non-monotonic behavior
  - Honest actions invalidate past security evidences
- Proportional burden
  - Retail & institutional traders vs HFTs

FuturesMEX Hybrid Solution

Confidentiality + Integrity
- Commitments + zk-proofs

Anonymity
- Anonymous network + Merkle tree
- Spent/unspent tokens

Non-Monotonicity
- Memoization
- MPC only in checking positions

→ *also solves Proportional Burden*

Beyond secure-with-abort
- Penalize aborting parties

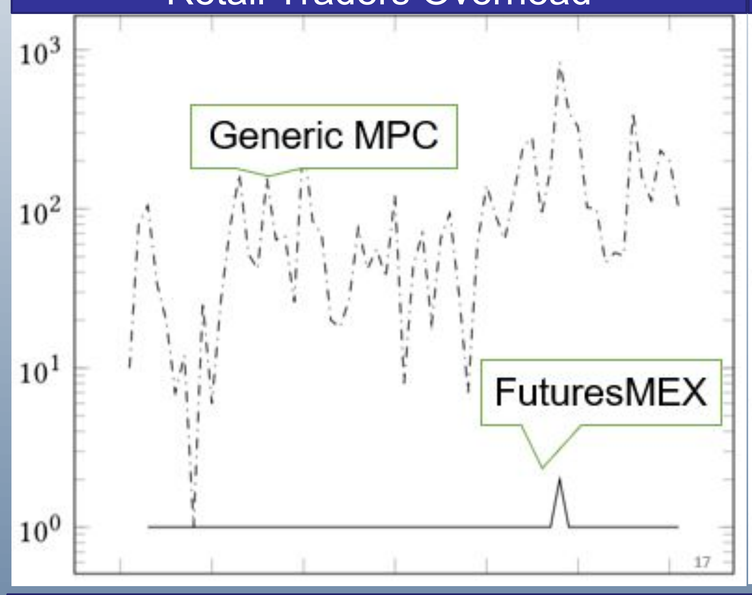
Further info: http://bit.ly/FuturesMEX

TSX Market → 300K Orders a Day

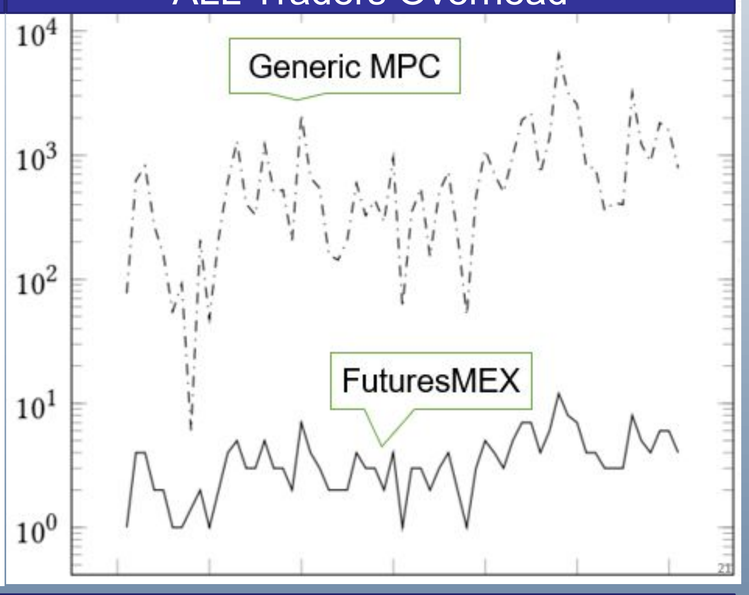
# of traders: HFTs are 29% comparing to 71% of retail and institutional Investors: 71%
# of orders: HFTs post 82%, of which 99% are limit orders (never to be executed)
Should normal investors pay for speculators?
This would happen if you just use MPC!!!

Compare on REAL data: Lean-Hog Q1-17

Retail Traders Overhead



ALL Traders Overhead



Take Away

Distributed financial protocols are desirable, but …
- Financial protocol is not always monotonic
- Viable protocol requires crypto effort proportional to activities

FuturesMEX is feasible for low-frequency market

Email: channam.ngo@unitn.it

Nam Ngo is a PhD Candidate/Research Fellow in the DISI Security Research Group at the University of Trento, Italy. He is working on Security Protocols for Distributed FinTech.