FuturesMEX

Secure, Distributed Futures Market Exchange

Fabio Massacci

University of Trento, Italy

*Joint work with **Chan Nam Ngo**, Jing Nie, Daniele Venturi, Julian Williams*

Some of this work is subject of the following patent applications
US62/625,428 PG448130GB

Outline

- What this is all about?
- Futures trading
  - Exchange functionality
  - Motivation & challenges
- Solution
- Evaluation

The Talk Message in a Slide

- In standard security we have
  - Good Guys, Bad Guys and
  - Failures → caused by Bad guys (or by "Good" guys who ain't so Good)
- More Good Guys join → old Good Guys still Good
  - So are their security proofs, credentials and all that
- Distributed FinTech is not like that
  - You have "honest failures" → economics forces security to be non-monotonic
  - And this has MAJOR implications for security design
- Key Intuition → Security Protocol Workshop 2018
- Full solution for Chicago Mercantile Exchange → IEEE Symp S&P 2018

Futures market as illustrative of FinTech

- A double auction market
- Bidders on both buy/sell side
- Futures contract
  - standardized promise to buy/sell barrels of oil, bushels of corn, …
  - made today and to be fulfilled in a future date
  - with cash reserve to meet promises
- Exchange platform for trading activities
  - Chicago Mercantile Exchange → centralized
- Other applications → Invoice Factoring (UNBIAS project)

How futures trading works?

Trader	Promises	Cash
Alice	0	1200
Bob	0	1500

Market price = 10$

Alice sells 100 promises

Bob buys 100 promises

Trader	Promises	Cash at the exchange
Alice	Buy 100	2200=1200+**100***10
Bob	Sell 100	500=1500-**100***10

At end of (trading) day
Market price = 8$

Promises must be fulfilled at end of day price:
Bob must sell and Alice must buy from the market

Trader	Promises	Cash at the exchange
Alice	~~Buy 100~~	1400=2200-**100***8
Bob	~~Sell 100~~	1300=500+**100***8

Alice made a profit of 200$, Bob lost.

Centralized futures trading (2)

Trader	Promises	Cash
Alice	0	1200
Bob	0	1500

Market price = 10$

Alice sells 100 promises

Bob buys 100 promises

Trader	Promises	Cash at the exchange
Alice	Buy 100	2200=1200+**100***10
Bob	Sell 100	500=1500-**100***10

At end of day
Market price = 12$

Trader	Promises	Cash at the exchange
Alice	~~Buy 100~~	1000=2200-**100***12
Bob	~~Sell 100~~	1700=500+**100***12

Promises must be Fulfilled at current price

Bob made a profit but Alice lost 200$

Market price is volatile

Trader	Promises	Cash
Alice	Buy 100	2200
…	…	…

100 promises to buy when price was at 10$ looked a good idea but things change

Hi Alice, can you deposit more money?

No? → Alice is liquidated.

Alice's cash reserve is now at 0$
→ ***Exchange must do something***

2200 > 12*100

2200 > 17*1000

2200 = 22*100!!!

12 17 22

If price rises further Alice's going broke

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ.

The purposes of the exchange?

- Publish the order book
  - Aggregate all orders
  - Protect traders anonymity
- Match orders
- Manage risks
  - Price oscillates
  - Retail and Institutional Traders
  - High frequency traders (HFTs)

	500 @ 20$
Sell	
	400 @ 16$
Market price = 11$	1000 @ 12$
	900 @ 10$
Buy	
	600 @ 8$
	700 @ 7$

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 8

The purposes of the exchange?

Publish the order book

- Aggregate all orders
- Protect tra[illegible]rs anonymity

Match

M[illegible]

Eurodollar (hi. freq.)
traders = 520
orders = 300K+
matches = 8402

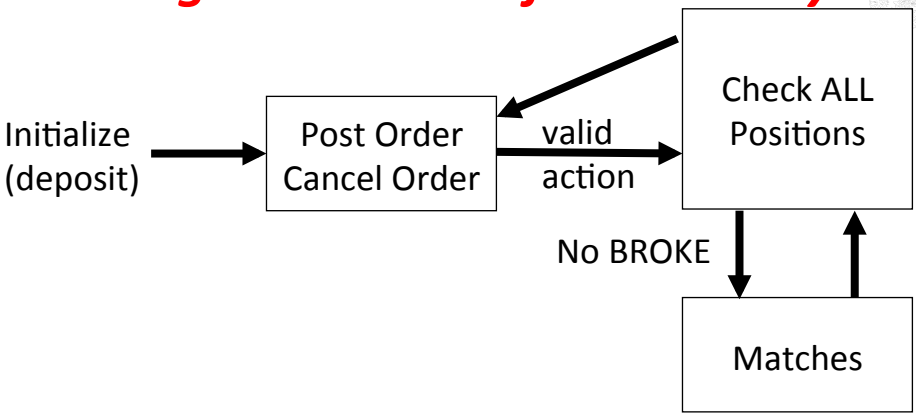
Lean Hog (low freq.)
traders = 33
orders = 6709
matches = 536

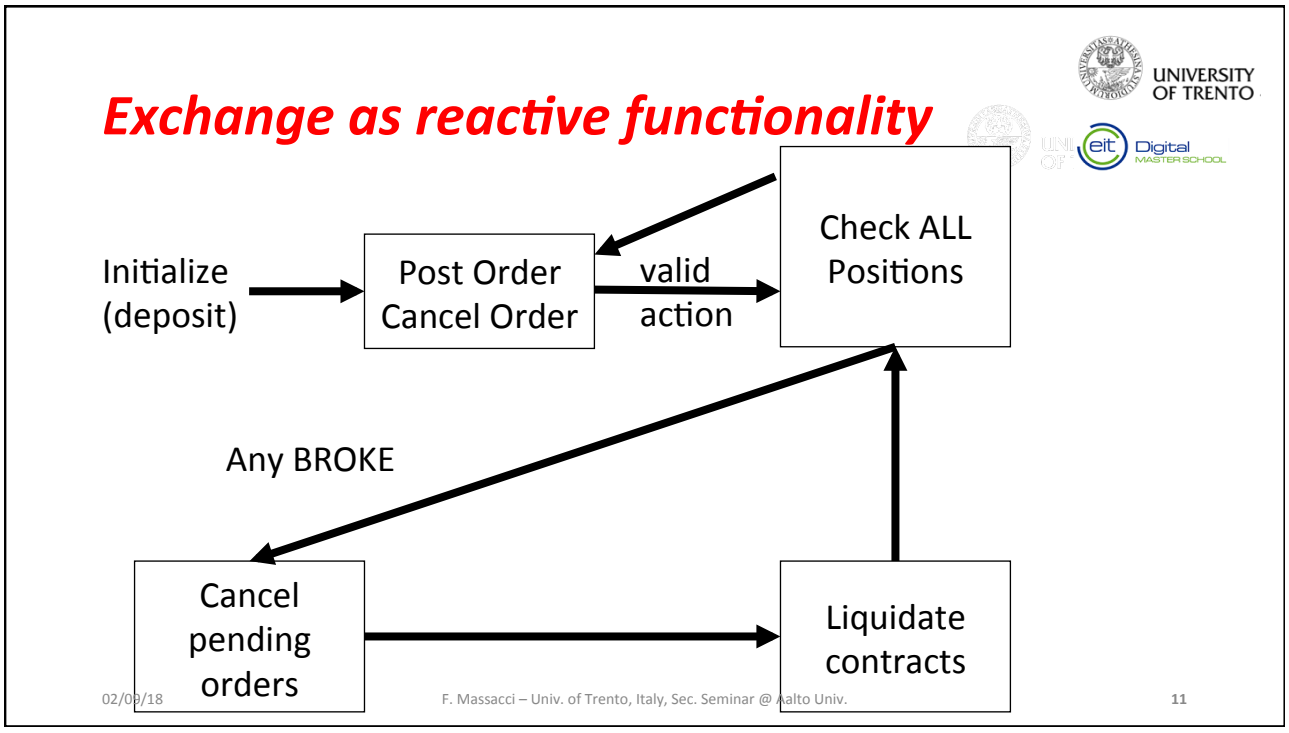
Market price = 11$

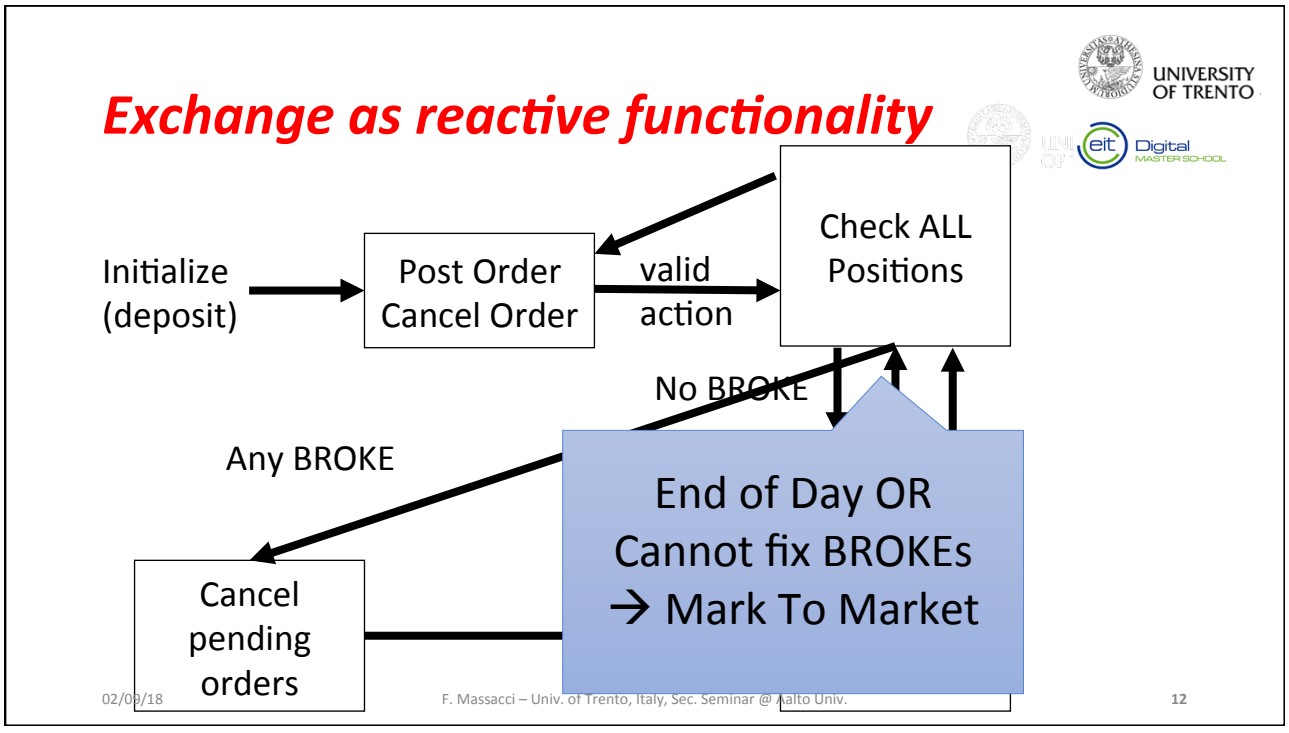
Buy

900 @ 10$
600 @ 8$
700 @ 7$

Exchange as reactive functionality




Exchange as reactive functionality
UNIVERSITY OF TRENTO
Digital MASTER SCHOOL
Initialize (deposit)
Post Order Cancel Order
valid action
Check ALL Positions
Any BROKE
Cancel pending orders
Liquidate contracts
02/09/18
F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ.
11


Exchange as reactive functionality
UNIVERSITY OF TRENTO
Digital MASTER SCHOOL
Initialize (deposit)
Post Order Cancel Order
valid action
Check ALL Positions
No BROKE
Any BROKE
End of Day OR
Cannot fix BROKEs
→ Mark To Market
Cancel pending orders
02/09/18
F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ.
12

FuturesMEX

- Replace centralized exchanges
- To allow buy and sell promises based on limited cash reserve
- Enforce trading discipline
- Protect market integrity

Technical challenges

- 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

ALL come as a package, or NOTHING will work individually.

Confidentiality & Price Discrimination Atttacks

UNIVERSITY OF TRENTO

T	Promises	Cash	Position
A	Buy 90	1000	100
B	Sell 30	1200	1500
C	Sell 30	1200	1500
E	Sell 30	1200	1500

IF E knows
1. A is tight in cash
2. A must buy 90 contracts
→ Can E bankrupt A ?

Market price = 10$

Buy	Sell
-	E: 20 @ 14
	C: 10 @ 11
B: 20 @ 9	-
A: 90 @ 8	-

Confidentiality & Price Discrimination Atttacks

UNIVERSITY OF TRENTO

UNI OF eit Digital MASTER SCHOOL

T	Promises	Cash	Position
A	Buy 90	1000	100
B	Sell 30	1200	1500
C	Sell 30	1200	1500
E	Sell 30	1200	1500

E's evil scheme:
→ Push price to 11.5$
→ Convince C to cancel

Market price = 10$

Buy	Sell
-	
	~~C: 10 @ 11~~
B: 20 @ 9	-
A: 90 @ 8	-

Market price = 11.5

T	Promises	Cash	Position
A	Buy 90	1000	***-35***
B	Sell 30	1200	1545
C	Sell 20	1310	1550
E	Sell 40	1090	1540

Confidentiality & Price Discrimination Atttacks

T	Promises	Cash	Position
A	Buy 90	1000	100
B	Sell 30	1200	1500
C	Sell 3	1200	1500
E	Sel	1200	1500

E's evil scheme:
→ Push price to 11.5$
→ Convince C to cancel

ONLY works if E knows A's exact position
Confidentiality is (technically) essential

T	Promises	Cash	Position
A	Buy 90	1000	-35
B	Sell 30	1200	1545
C	Sell 20	1310	1550
E	Sell 40	1090	1540

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 18

Non-Monotonicity: What's different from other crypto protocols?

- In all security protocols we are used to
  - All good guys do the same thing!
  - And they all do it once!
- Authentication
  - Alice wants to be authenticated by a TLS server
  - And so does Bob I, and Bob II, and Bob III, and Bob IV
- E-Voting → Alice casts 1 vote, and so Bob I, Bob II,
- Auctions → Alice makes 1 bid, and so Bob I, …
- Reputation Systems → Alice posts her rating, and so does Bob I, Bob II, Bob III, …

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 19

Enter Ditributed FinTech

- Fat cat Sam is gone → only Alice and the Bobs
- Alice trades in Barrels of Oil with the Bobs
  - Commits she'll buy B barrels at the end of the day
  - Proves in ZK she has cash $>B*P to buy them at current price P
  - Bob III agrees to sell her B barrels at whatver end price
- All is good and the Bobs making offers
- Seems pretty similar to good old protocols…

Futures market is non-monotonic

App.	Honest move	Affect what?
Payment system	A does nothing, B sends X coins to C	B, C's balance
E-Voting	… , B casts a vote	B's vote
Reputation	… , B does something	B's reputation
Futures market	A does nothing, B posts an order, --> Market price changes	ALL positions including A's → A can become BROKE

Futures market is non-monotonic

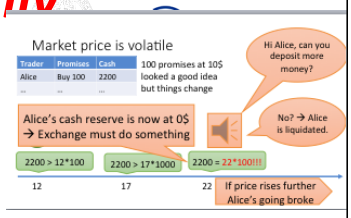
App.	Honest move	
Payment system	A does nothin B sends X coir	
E-Voting	… , B casts a v	
Reputation	… , B does sor	
Futures market	A does nothing, B posts an order, --> Market price changes	ALL positions including A's → A can become BROKE

Non-monotonic:
A does NOTHING but A's crypto evidence of good standing is invalidated by B's action (a good guy)

Why is This important? Technically

- We want to get rid of fat cat Sam doing financial intermediation → MPC of Alice and the Bobs
- Since MPC is costly → Replace MPC by ZK proofs → all asynchronous
  - Alice proves in ZK she is in good standing and sends it off
  - Bob I proves in ZK he is in good standind and sends it off
  - Bob II proves in ZK he is in …
  - They can verify all that asynchronously
  - Minimize MPC step to the crypto magic at the end
- A LOT MORE EFFICIENT → BUT MONOTONICITY NEEDED
  - Bob VIII won't make Alice claims invalid

Why is This Important? Economically



- Fat cat Sam is gone
- Alice committed to buy from Bob III
- Enters Good Bob VIII
  - He wants to buy more oil → price surges
  - What happens to Alice? Has she cash enough?
  - Sam would call Alice to make sure she pour cash if price rises but Sam's gone
  - Who is giving Bob III the money? Sam would but… Sam's gone and Alice can't foot the bill…

Why is This Important? Combined…

- Bob VIII did a honest protocosl
  - He is perfectly honest and make a perfectly valid ZK
  - But he bankrupted honest Alice
- All Alice ZK proofs, committment credentials were
  - economically and crytptographically-valid (then)
  - but economically invalid (now)
- Monotonicity is destroyed → so is the possibility to replace MPC with straightforward ZK → need ad-hoc protocols

Solution Overview

- Confidentiality + integrity
  - Commitments + zk-proofs
- Anonymity
  - Anonymous network + Merkle tree
  - Spent/unspent tokens
- Non-monotonicity
  - Memoization
  - MPC only in checking positions

Check ALL Positions

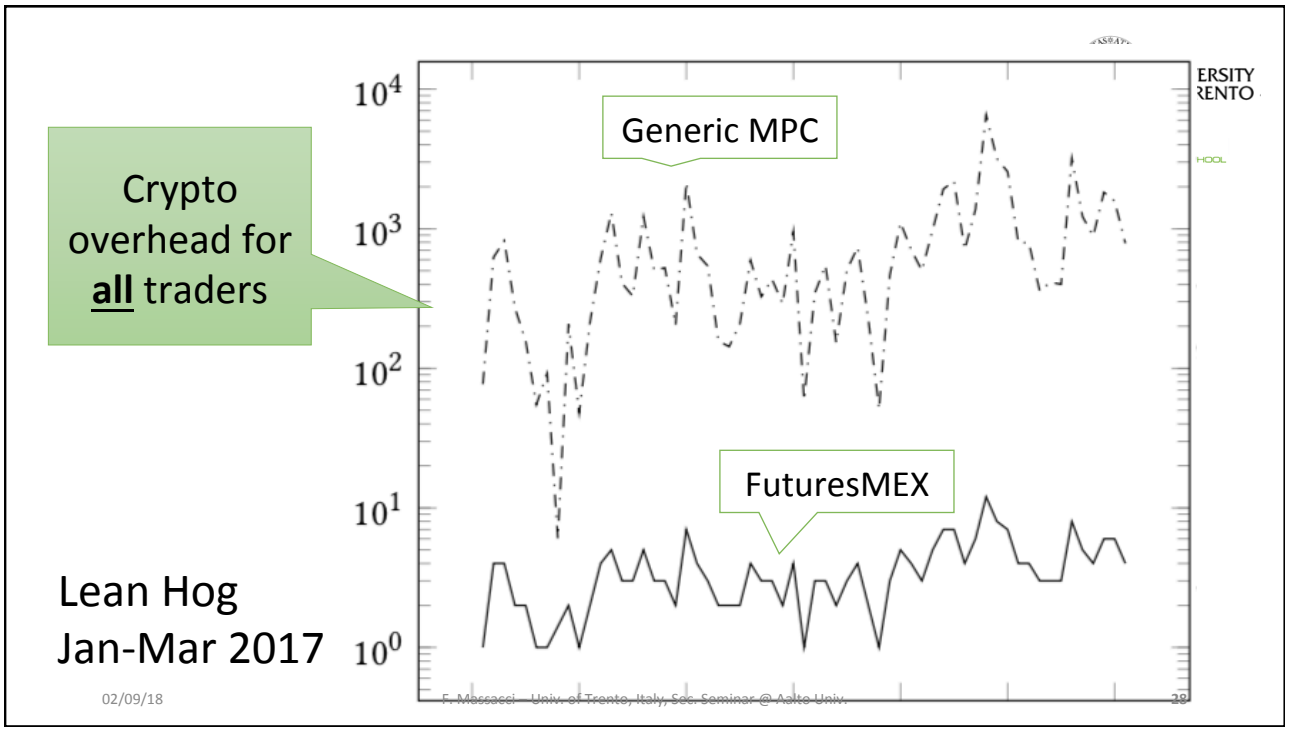
MPC to hide # of BROKE traders

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 26

The Armchair Cryptographer Alternative

- Well, why bother???
  - Just run General MPC and job done
  - We know from the Sugar Beet Danish auction back in 2008 that MPC can stand thousands parties so what's all that fuss?
- Questions:
  - Who actually read the sugarbeet auction paper?
  - 1229 farmers joined but how many Alices and Bobs (in security terms) joined the MPC protocol?

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 27



Ok, MPC is expensive, but…

- That's the price for getting rid of middleman Sam
- Could we implement every step with MPC?
- Yes, but… everybody would do the same computation --- making 1 or 1000 orders
  - Alice and the Bobs are in the same boat aren't they?
  - Well, Some Bobs are "slightly" more active…

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 29

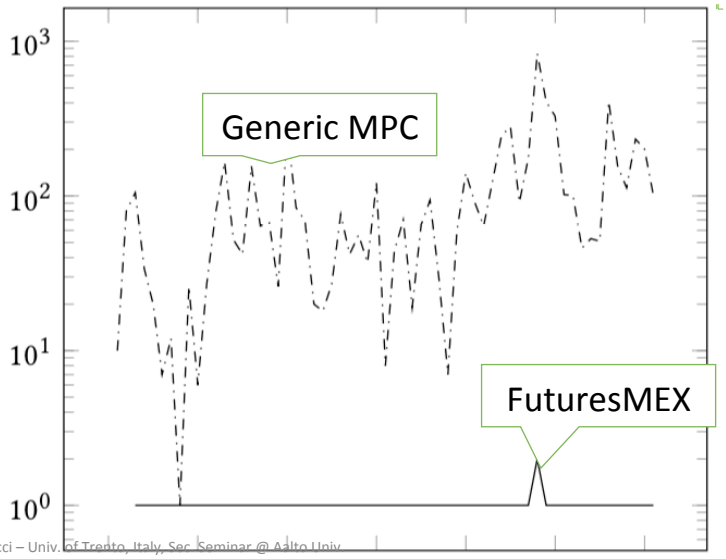
Frantic Alice and the Sleepy Bobs

- TSX Market → 300K orders per day
  - 71% are Retail and Institutional Traders
  - 29% are Algorithmic Traders
- Proportions of orders
  - 82% of 300K orders by Algorithmic Traders
  - 99% of those orders are limit orders → never to be matched in an actual trade
    - Basically away from the current price
- But in MPC everybody does the same…

Our hybrid protocol

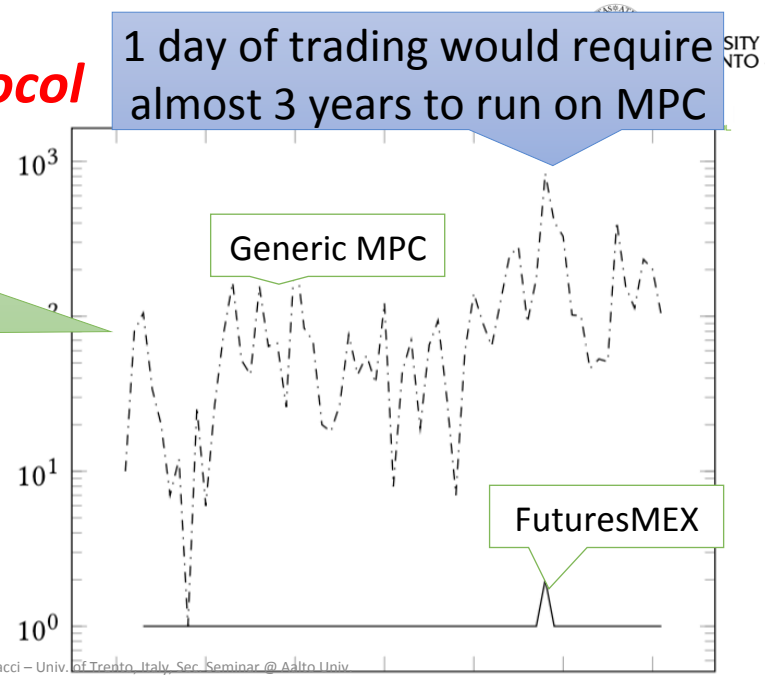
- Use mostly zk-proofs
  - Traders posting order
  - → must prove
  - Passive traders
  - → only verify
- Only use MPC for checking positions

Lean Hog
Jan-Mar 2017



Our hybrid protocol

- Crypto overhead for **retail** traders (**few** orders, mostly **passive**)
  - Passive traders
  - → only verify
- Only use MPC for checking positions



02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ.

Beyond security-with-abort

- Malicious party can abort
  - Not joining MPC, not proceeding to match
- Can we stillmark to market?
- We need to penalize the mailcious party
- How?

Claim-or-refund [Kumaresan 2016] ***NO*** → Uneven amount of deposit

Lock-then-release [Kosba 2016] YES → Just lock the initial cash

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 33

Beyond security-with-abort (cont)

- Malicious party can abort
  - Not participate in MPC, not proceed to match
- Can we still mark to market?
- We can also penalize the malicious party
- Lock-then-release by [Kosba 2016]
  - Lock the initial cash
  - To join the mark to market → prove you did what you should have done it
  - Else lose the deposit & divide money among others

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 34

Evaluation + Optimizations

Action	Trader	Others
Init	11s	-
Post	39s	148s
Match	29s	148s
Mark	28s	-

↓

Action	Trader	Others
Post	24s	27s
Match	26s	27s

Timing on AWS Large (128GB RAM Instance)

Many **intermediate** commitments
Streamline the **# of commitments**
→ Reduce zk-proof gen time

Combine **MPC + penalty**
1. MPC **without** consistency check
2. If there are broke traders, pick 1 volunteer to prove
1. If there are no broke traders, everyone prove

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 36

Evaluation + Optimizations

Action	Trader	Others
Init	11s	-
Post	39s	148s
Match	29s	148s
Mark	28s	-

Timing

Final MPC step with consistency checks

Combine **MPC + penalty**

Action	Trader	Others
Post	24s	27s
Match	26s	27s

Light MPC step + penalty
Optimized zk-proofs gen

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 37

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
- There is more to do !!!
  - Hi-frequency market, e.g Eurodollar?
  - Dropout tolerant?
  - Dark pool: orders only visible conditionally

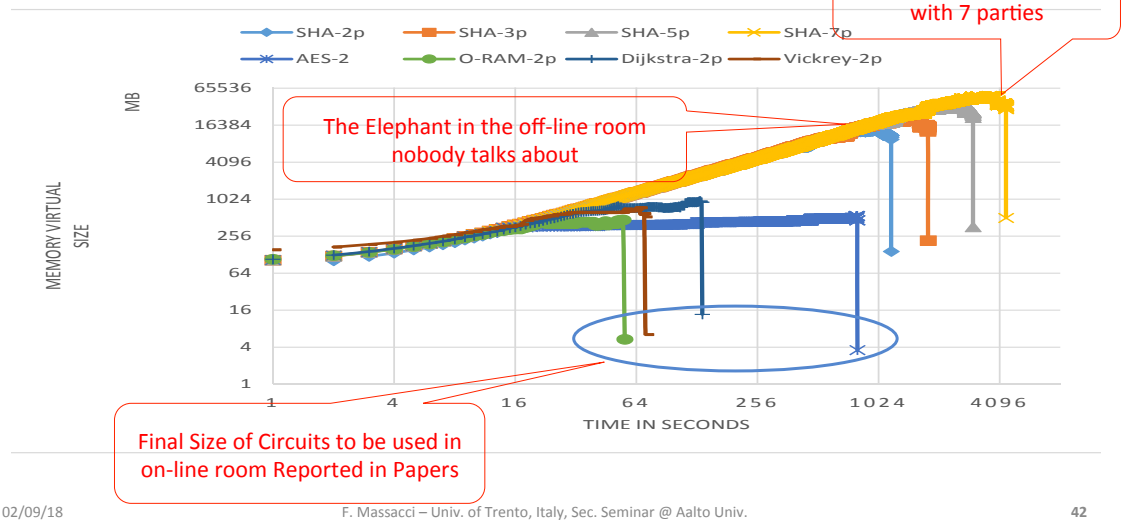
02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 39

Acknowledgement

- Part of our research on FinTech and Blockchains has received funding from the European Institute of Innovation and Technology (EIT) thorugh the UNBIAS Project of EIT Digital.
- This body of the European Union receives support from the European Union's Horizon 2020 research and innovation programme.

Bonus Material

Limits of "effective" MPC (SPDZ)



02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 42

Well, it's off-line, so what?

- IF you only vote ONCE or you only bid ONCE then it is off-line
- If every time "yet another Good Bob" does something Alice and the Bobs need to run an MPC round, well, it ain't "off-line" anymore
  - For example if they need check Bob VIII bid didn't bankrupt Alice and so Bob IX and so Bob X…
  - And you can't recycle the off-line part (unless you're so green to recycle also one-time pads…)

02/09/18 F. Massacci – Univ. of Trento, Italy, Sec. Seminar @ Aalto Univ. 43