UNIVERSITY OF TRENTO

Complexity, Cryptography, and Financial Technologies

Lecture 4 – Security Requirements for FinTech Cases

Fabio Massacci

Illustrative Cases

UNIVERSITY OF TRENTO

- **We use these two case studies for later project development**
- **Futures Market Trading**
  - Trading Scenario in which traders buy and sell financial instruments but must have cash to backup their bids e.g. Chicago Mercantile Exchange
    - More well known for Eddie Murphy and Dan Akroid Movie
    - *https://www.youtube.com/watch?v=v9JcJgXATU8*
- **Invoice Factoring**
  - Financing activites in which companies bring a invoice to banks to receive an advance payment before the buyer settles (but should not present the same invoice twice)

Futures market as illustrative of FinTech

UNIVERSITY OF TRENTO

- **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

Futures - Example

UNIVERSITY OF TRENTO

- **Simple derivative contract.**
  - A promise to deliver an asset position (buy or sell) a specific date for a specific price.
- **Example:**
  - WTI Crude Futures, "CLM2", each contract is a buy or sell claim for 1,000 barrels of West Texas Intermediate (CL) crude oil on the third Wednesday of June (M) in the year 2022 (nearest future year ending in 2), the maturity date.
- **Two types of settlement to imbue value on the contract:**
  - Daily Settlement, all outstanding positions converted to cash at current price.
  - Final Settlement, all outstanding contracts open on Friday prior to maturity date are settled by agreeing to exchange the physical commodity: the barrels of oil
- **Majority of futures contracts are settled as a cash difference**
  - between a reference price and the final price of the traded contracts just prior to the maturity date.
- **They can be combined:**
  - "We want to fix a forward position in June 2022 for an asset
  - We need to hold long June 2022 contracts
  - We can partly finance this position by shorting, short maturity contracts etc."
    - I want to actually sell oil in June, maybe price fluctuates and I'm in trouble, so I get and keep a promise (by somebody else) to buy my oil at a good price, to pay for this position I use promises to sell back the oil in short term as the price fluctuates
    - I'll sell the day after tomorrow, I'll buy it tomorrow for the price of the day after tomorrow

How futures trading works?

UNIVERSITY OF TRENTO

Trader	Promises	Cash
Alice	0	1200
Bob	0	1500

Alice sells 100 promises

Bob buys 80 promises

Trader	Promises	Cash at the exchange
Alice	Buy 100	2200=1200+**100***10
Bob	Sell 100	700=1500-**80***10

Market price = 10$

At end of (trading) da
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 80~~	1360=700+**80***8

Alice made a profit of 200$, Bob lost.

5 19/09/18

Centralized futures trading (2)

UNIVERSITY OF TRENTO

Trader	Promises	Cash
Alice	0	1200
Bob	0	1500

Alice sells 100 promises

Bob buys 80 promises

Trader	Promises	Cash at the exchange
Alice	Buy 100	2200=1200+**100***10
Bob	Sell 80	700=1500-**80***10

Market price = 10$

At end of day
Market price = 12$

Promises must be Fulfilled at current price

Trader	Promises	Cash at the exchange
Alice	~~Buy 100~~	1000=2200-**100***12
Bob	~~Sell 80~~	1660=700+**80***12

Bob made a profit but Alice lost 200$

6 19/09/18

Market price is volatile

Trader	Promises	Cash
Alice	Buy 100	2200
…	…	…

100 promises to buy wh 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

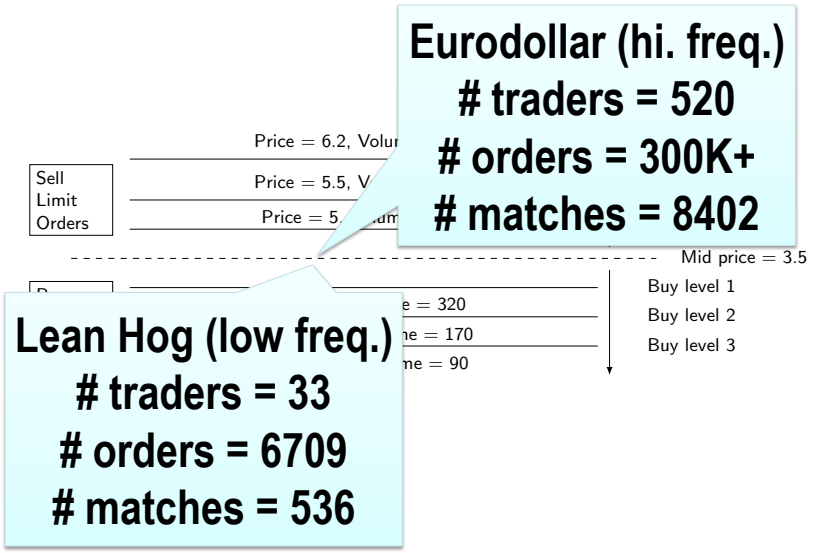
7 19/09/18

How does The Exchange Keep Track?

- **The Limit Order Book**
  - Auction mechanism that facilitates trade of assets and provides benchmark prices accessible to ALL members of the market.
  - Traders post buy and sell orders and the clearing of these orders forms part of the purpose of the limit order book.
- **Two types of orders:**
  - Limit orders (quotes), that specify a price and volume at which the trader is willing to buy or sell an asset.
  - Market orders, a request to buy or sell an asset
- **The limit order book displays current set of limit orders and records the execution of market orders as traded prices.**
- **A critical feature of the limit order book is that part of the order book is public (information visible to all traders) and part is private.**

Example of the public part of the order book

UNIVERSITY OF TRENTO

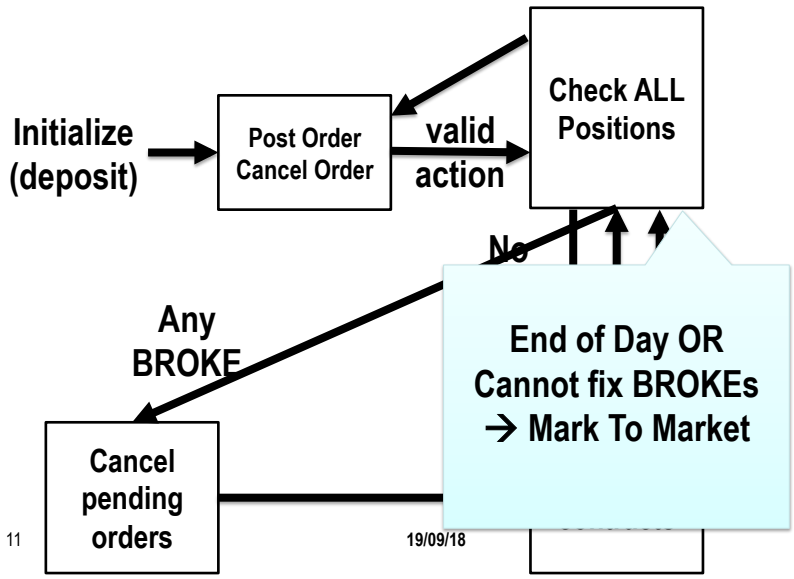


Summary View of Futures Trading

UNIVERSITY OF TRENTO

- **Future Contract**
  - Essentially a standardized bet on the value some uncertain quantity, usually a traded asset, such as a stock or commodity price.
- **Centralized Clearing House**
  - Essentially a casino allowing traders to take positive (bet on an increase) and negative (bet on a decrease) positions.
  - The stock or commodity price like a roulette wheel generating random outcomes on which traders bet
  - Traders must buy chips in advance before being able to place bets and must bet within the limits of their chips (cash margin)
- **Key Functionalities of the Clearing House**
  - acts as a trusted third party monitoring each trader to ensure they have sucient funds to maintain their positions.
  - runs the continuous auction that allows traders to post limit orders (quotes) and execute market orders (trades).
  - If a trader cannot maintain their position through lack of funds the clearing house `margins' him, i.e. clears the account using currently available quotes to determine the price.

Exchange as reactive functionality



Now we want to make it distributed

- **Easy to see**
  - Market integrity
  - Consensus (synchronization)
- **Your Call?**
  - Size → blockchain is going to be veery big
  - Efficiency → what if you don't have enough capacity
  - Anonimity - confidentiality?
    - Can't have, you need to know the amount of money for every transactions or at least current one
    - Need to send the oil to someone and even the amount of oil to send
  - Audit log?
  - - what is a node go off line while some key trades for him take place?
  - Concurrency rush + Market fluctations asynchronously

Now we want to make it distributed

UNIVERSITY OF TRENTO

- **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.

13 19/09/18

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 ?

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

11.5

14 19/09/18 F. Massa cci –

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

UNIVERSITY OF TRENTO

- **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, …**

Enter Distributed FinTech

UNIVERSITY OF TRENTO

- **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 *c*>*p***b* to buy them at current price *p*
    - We don't know yet how ZK works, but it is just enough to know that cryptomagically she can convince somebody of a secret without revealing it
  - Bob III agrees to sell her *b* barrels at whatever end price
- **All is good and the Bobs keep making offers**
- **Seems pretty solid…**

Futures market is non-monotonic

UNIVERSITY OF TRENTO

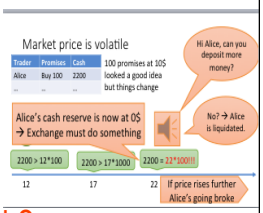
App.	Honest move	
Payment system	A does nothing, B sends X coins to C	
E-Voting	… , B casts a vote	
Reputation	… , B does something	[illegible]
Futures market	A does nothing, B posts an order, --> Market price changes	ALL positions including A's → A can become BROKE

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? Economically

UNIVERSITY OF TRENTO

- **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…
- **Also has major technical implications**
  - we will see them after you know more about ZK and MPC



The Proportional Burden Requirement

UNIVERSITY OF TRENTO

- **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
- **Protocols must make sure that a node "pays" (either financially or computationally) in proportion to its level of activity**
  - Otherwise why on earth an institutional investor should spend money to run a blockchain node so that a speculator can make carzy bids???

More Requirements

UNIVERSITY OF TRENTO

- **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**
- **How to do it?**

Forcing Losing Parties to Join

UNIVERSITY OF TRENTO

Claim-or-refund [Kumaresan 2016]

- To play for a cash amount X
- Lock cash
  - in proportion to the number of users before your turn (nX)
- When it is your turn you do what you should do → your deposit is unlocked
- Else lose deposit and money divide

Lock-then-release by [Kosba 2016]

- To play for a cash amount X
- Lock cash
  - same value X for everybody
- Prove you did what you should have done it → your deposit is unlocked
  - Requires a ledger on which everybody else will only give you the money back if you comply with your own contract
- Else lose the deposit & divide money among others

Factoring Invoices

UNIVERSITY OF TRENTO

- Factoring Invoices is a Completely Different Scenario
- The Scenario
  - Seller send invoices to Buyer for some job done
  - Buyer normally pays in 30, 60, 90 even 120 days
    - Italian public administrations even after years
- How can Seller pay his own suppliers, employees?
  - Owners are rich by family inheritance or
  - It goes to a “factor” (e.g. a bank) and get a cash advance
  - What if it goes to two banks with the same invoice?
- Distributed Ledger is natural solution

EU factoring turnover is 1.26 Trillion Euros in 2017

UNIVERSITY OF TRENTO

Country	Factoring market size '17 (in bln)	Average payment term '17	Percentage of sales made on credit '17	Average 'Days Sales outstanding' (DSO) '17	GDP penetration '16	Contribution of SMEs to Value added at factor costs '16
United kingdom	€326.9	23 days	45.7%	31 days	13.8%	51.8%
France	€268.2	34 days	29.3%	42 days	12.10%	54.5%
Germany	€216.9	24 days	26.5%	25 days	6.9%	54.1%
Italy	€208.6	50 days	42.5%	85 days	12.5%	67.7%
Spain	€130.7	45 days	37.8%	47 days	8.7%	61.8%
Netherlands	€82.8	24 days	35.0%	41 days	11.9%	62.9%
Europe tot/ average	€1256.7	31 days	38.8%	44 days	-	

Source: FCI annual review '17, EUF 2016, Atradius payment practice barometer 2017, Eurostat 2016

Current Market Structures

UNIVERSITY OF TRENTO

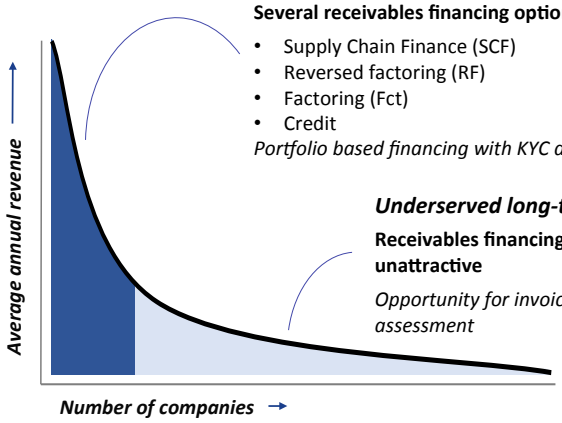
- **Who can benefit from a distributed ledger solutions?**

Focus of todays receivables financing market

Several receivables financing options available:

- Supply Chain Finance (SCF)
- Reversed factoring (RF)
- Factoring (Fct)
- Credit

Portfolio based financing with KYC driven risk assessment



Underserved long-tail of receivables financing

Receivables financing options very limited and unattractive

Opportunity for invoice based finance data driven risk assessment

24

Why this is interesting now?

UNIVERSITY OF TRENTO

- **NL situation**
  - Buyers currently often prevent sellers from factoring an invoice in their procurement terms
  - NL government intends to restrict this practice by law by end 2018
  - Consequently, SMEs will be able to attract working capital through factoring and factoring market is expected to increase
- **What can change**
  - In a factoring situation, the invoice must be settled with the Factor rather than the Seller. Because this is non-standard, it introduces a settlement risk.
  - We expect buyers to need solutions for prevention of wrongfully paid invoices, cumbersome rectification processes and potential loss of money.
- **If such solutions are successful, it can also increase single invoice factoring and outstanding invoice factoring.**

6

Security Requirements

UNIVERSITY OF TRENTO

- **Your Take (Full document describing case study on Classroom)**

19/09/18 Massacci, Ngo - Complexity, Crypto, and FinTech ► 26