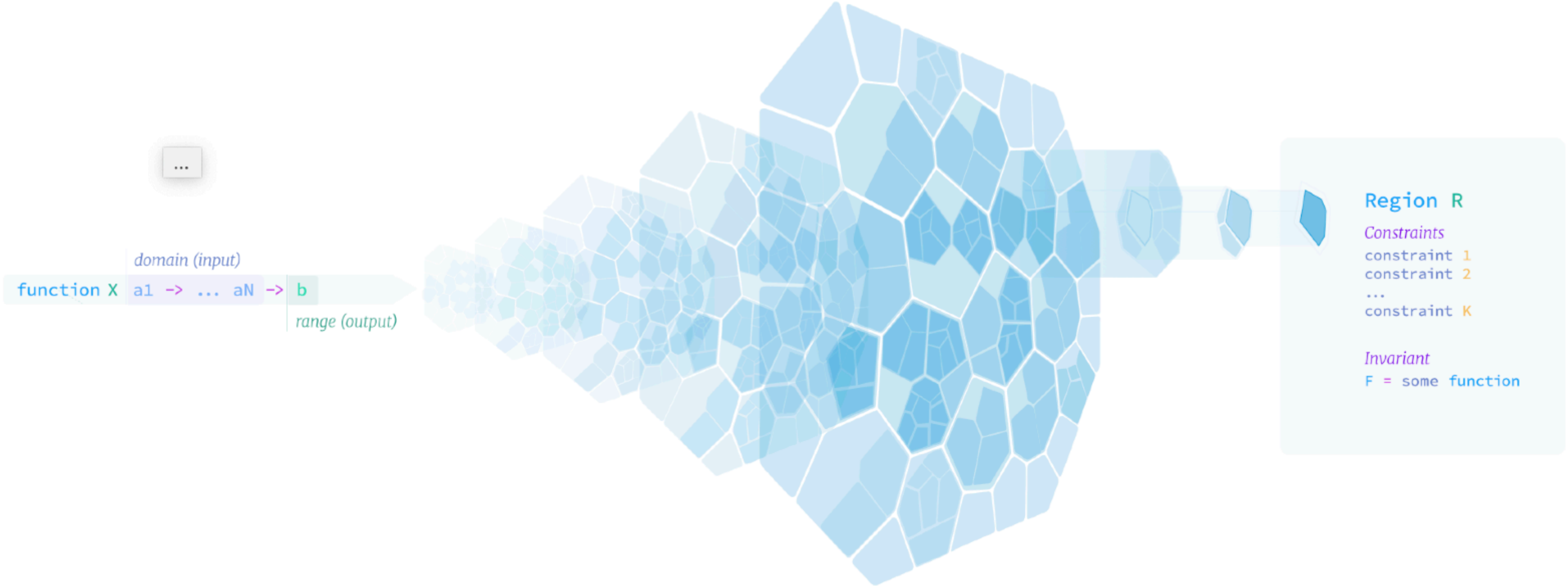
Formal Verification of Financial Infrastructure with Imandra



NSF Formal Methods in the Field
University of Iowa
November 13th, 2024

Grant Passmore
Imandra Inc, and
Clare Hall, University of Cambridge

Problem

Financial markets have become notoriously unstable.

Problem

Financial markets have become notoriously unstable.

Flash Crashes: systemic events characterised by non-trivial co-dependence of trading algorithms (e.g., May 2010, drop of $1tr)

Problem

Financial markets have become notoriously unstable.

Flash Crashes: systemic events characterised by non-trivial co-dependence of trading algorithms (e.g., May 2010, drop of $1tr)

Lack of Transparency: issues of misrepresentation (e.g., misleading marketing materials or regulatory filings) of trading algorithm behaviour (e.g., BATS/Direct Edge $14M settlement with the SEC)

Problem

Financial markets have become notoriously unstable.

Flash Crashes: systemic events characterised by non-trivial co-dependence of trading algorithms (e.g., May 2010, drop of $1tr)

Lack of Transparency: issues of misrepresentation (e.g. misleading marketing materials or regulatory filings) of trading algorithm behaviour (e.g., BATS/Direct Edge $14M settlement with the SEC)

Glitches: trading system errors in design or implementation, often causing significant losses (e.g., Knight Capital's loss of $400M)

Introducing Imandra

We are an AI company developing Imandra, an automated logical reasoning engine for analysis of algorithms.

We specialise in:

"**Automated Reasoning**"

- Machine analysis of systems
- Correctness and rigour
- Formal verification
- Safe AI

What we deliver:

- AI-based system transformation and governance
- **Lossless understanding** - a living digital record of your systems
- New business intelligence and revenue

We empower innovation:

Use the science of Automated Reasoning to:

- Transform change management
- Solve for operational resiliency
- Increase productivity

SELECT CUSTOMERS & PARTNERS

Goldman Sachs BlackRock. OneChronos UBS EURONEXT KPMG

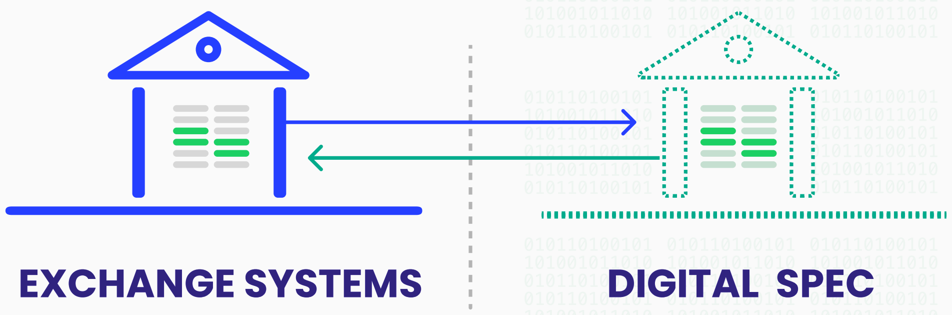
DARPA citi

Transform Exchange System Management

Use a Imandra Markets **to model, verify, test and supervise** your system.

Put the requirements into a digital spec

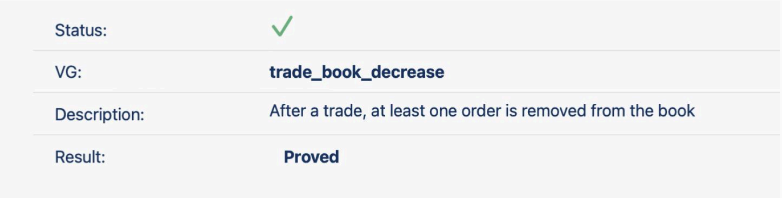
A single source of business requirements in a digital spec.
No ambiguity, no debate.



*We think of this as "**lossless understanding**" - a living digital twin of your system. Stop losing information as your systems age, developers move on, and documentation is under specified or worse still, non-existent.*

Prove key system properties

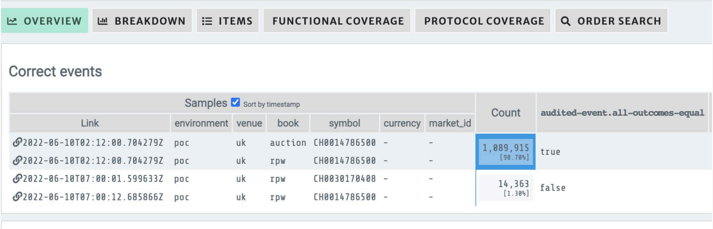
Scientific proof that regulatory obligations are met or identify where and how they fail.



Status:	✓
VG:	**trade_book_decrease**
Description:	After a trade, at least one order is removed from the book
Result:	**Proved**

Fast track and monitor progress

20x faster regression. Catch bad code and design.

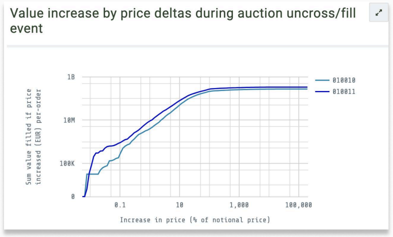


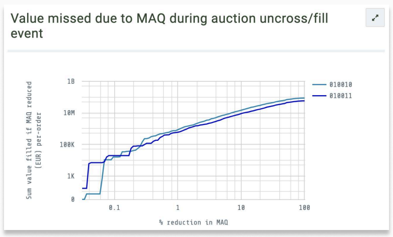
Correct events

Samples ☑ Sort by timestamp							Count	audited-event.all-outcomes-equal
Link	environment	venue	book	symbol	currency	market_id		
2022-06-10T02:12:00.704279Z	poc	uk	auction	CH0014786500	-	-	1,089,915 [98.70%]	true
2022-06-10T02:12:00.704279Z	poc	uk	rpw	CH0014786500	-	-		
2022-06-10T07:00:01.599633Z	poc	uk	rpw	CH0030170408	-	-	14,363 [1.30%]	false
2022-06-10T07:00:12.685866Z	poc	uk	rpw	CH0014786500	-	-		

System & Business Intelligence

New perspectives for you and your clients.


Value increase by price deltas during auction uncross/fill event


Value missed due to MAQ during auction uncross/fill event

The benefits for our Exchange customers

	Before		After		Value
Operational Resilience	**Hand-written**, **out-of-date**, partial documentation	→	**Formally verified *single source of truth***	→	**Lossless understanding.** Stakeholder alignment.
	No verification of **production data**	→	**Full daily audit** of all production data	→	**Full production supervision**
	>2 outages per month. Significant impact.	→	**<3 in five years**	→	Less downtime. Better reputation.
Productivity	**Manual regression** & unit tests - 4-week cycle	→	**Automated full functional suite - daily.** Regression. Stress. Failover.	→	**20x time save.** Full test coverage, every time.
	Monthly production deployment	→	**Weekly** release cycles	→	**4x time save**
	Basic management information	→	**Model-driven 'what if' actionable analytics**	→	Focus on **business growth**

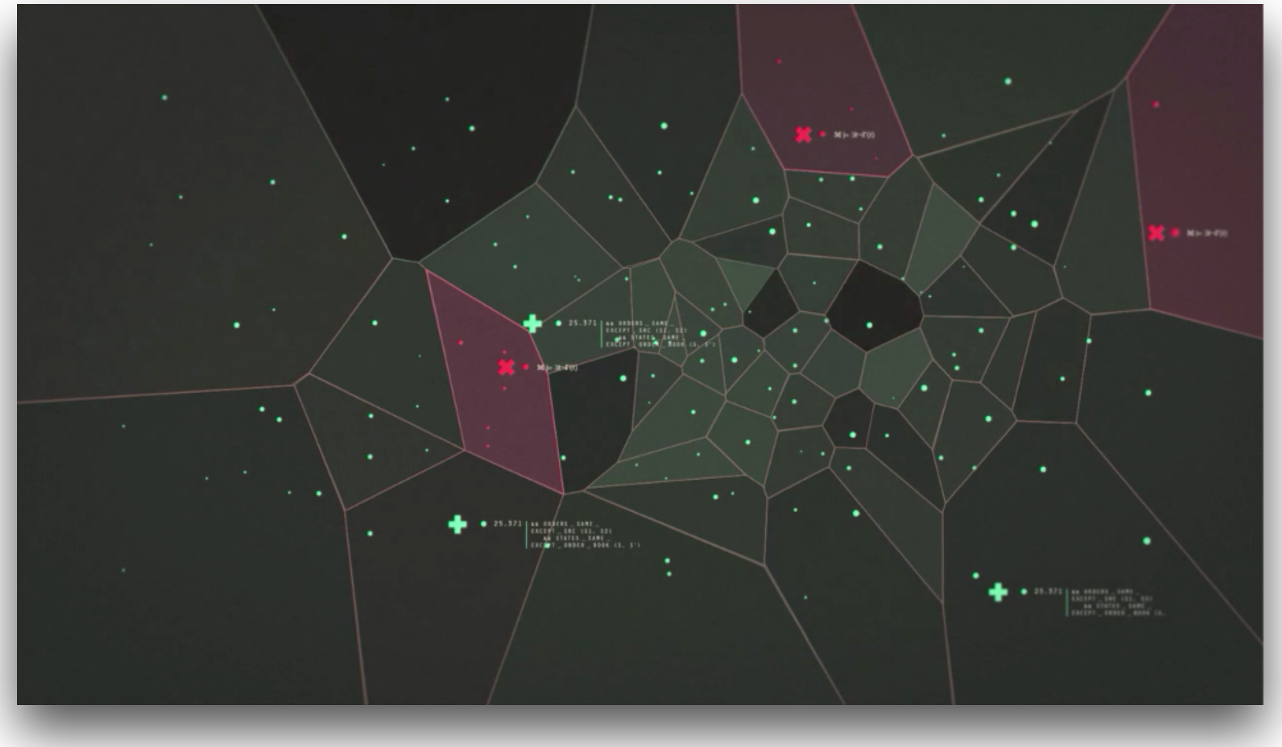
Our success

- >24% EU equity volume supervised by Imandra Markets
- Over 550 significant issues & regulatory breaches discovered.
- Proven with multiple clients on 9 large scale change programs.

What is Imandra?

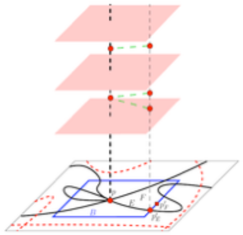
OCaml + Automated Reasoning

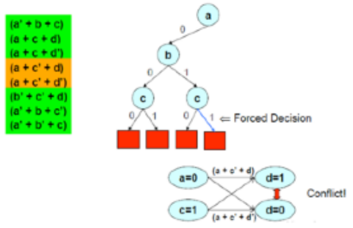
- Programming language
- Mathematical logic
- Reasoning engine

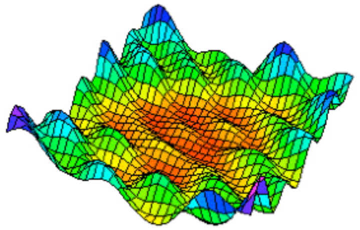


IMANDRA

REASONING AS A SERVICE™



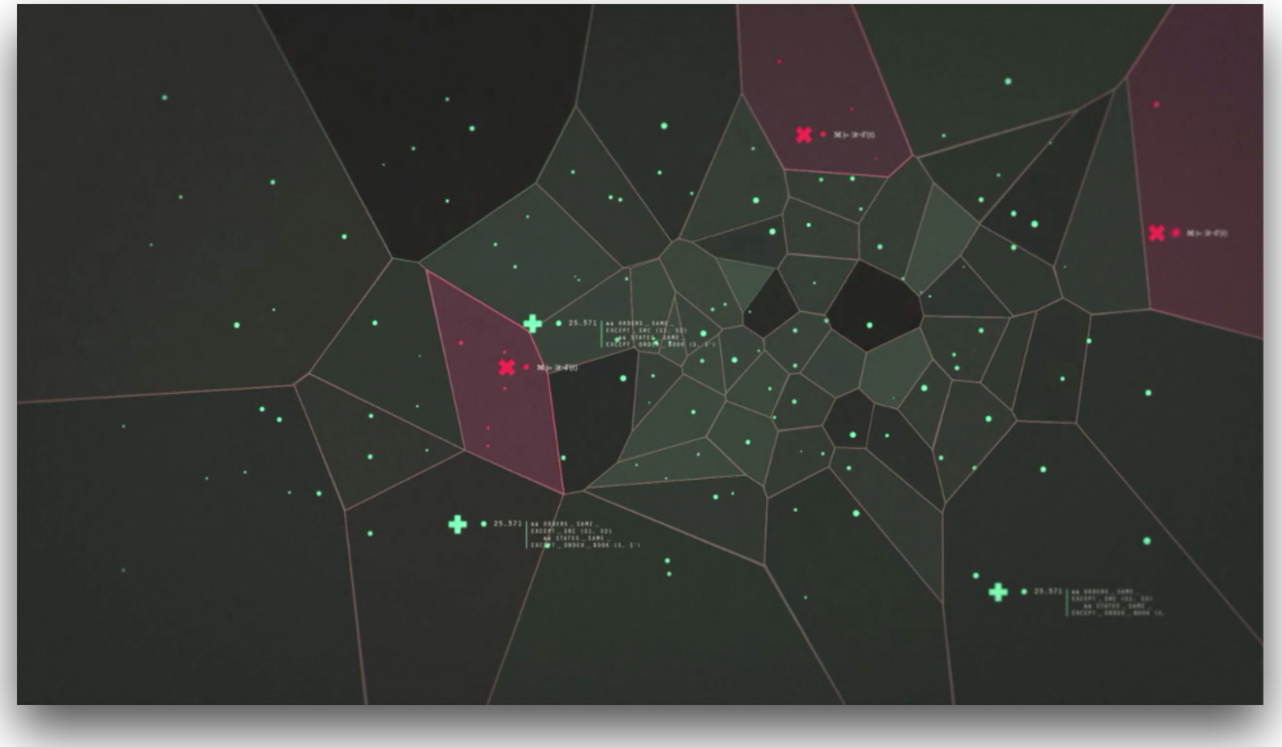




What is Imandra?

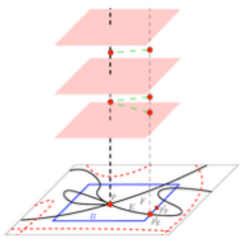
OCaml + Automated Reasoning

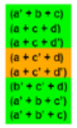
- Programming language
- Mathematical logic
- Reasoning engine
  - First-class counterexamples
  - Automated induction (epsilon_0)
  - Nonlinear region decomposition
  - Proof automation tailored to various algorithm regulations
  - Test suite generation & analysis
  - Model-based auditing framework
  - First-class state-space decompositions

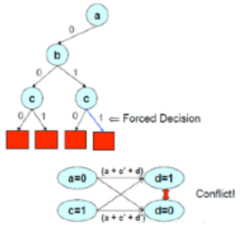


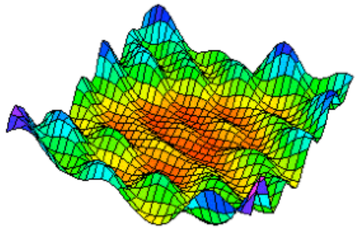
IMANDRA

REASONING AS A SERVICE™



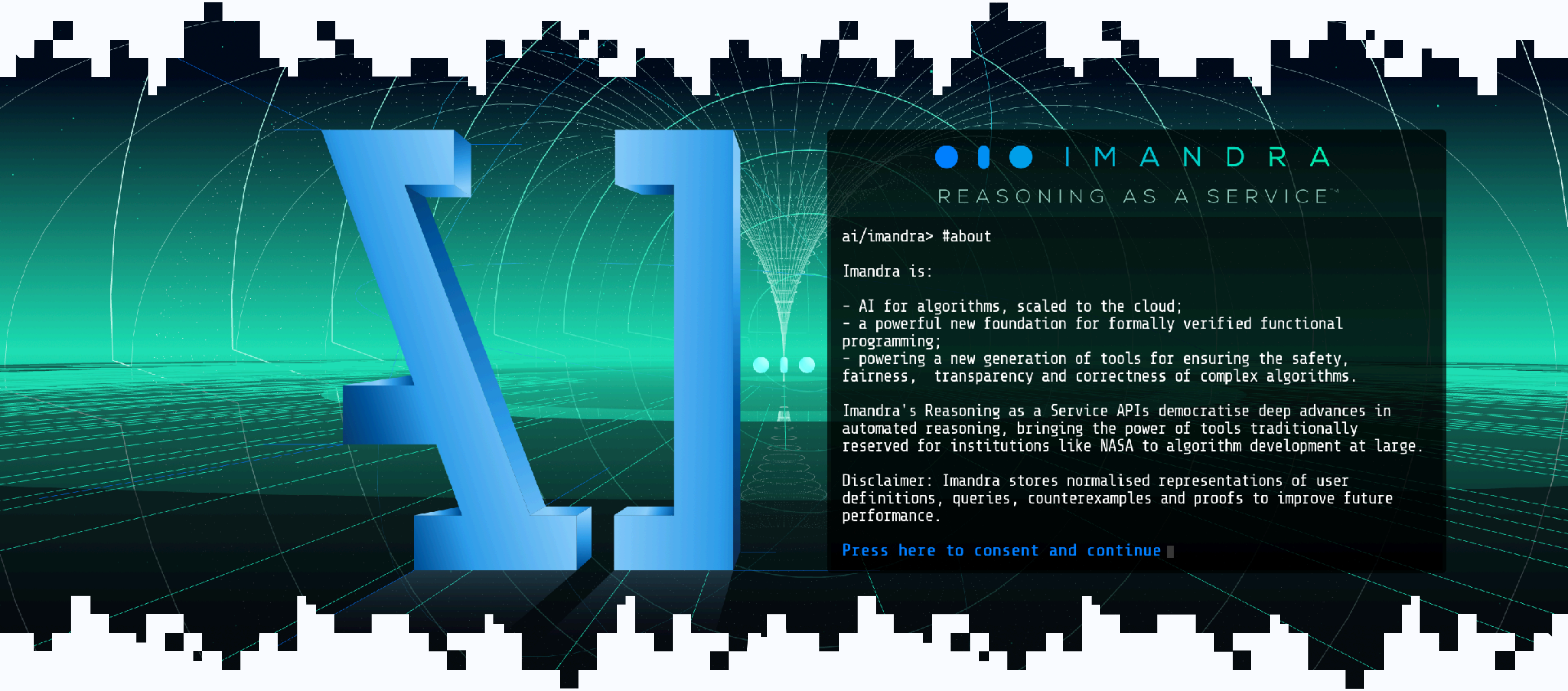






Try Imandra in the Cloud!

https://try.imandra.ai

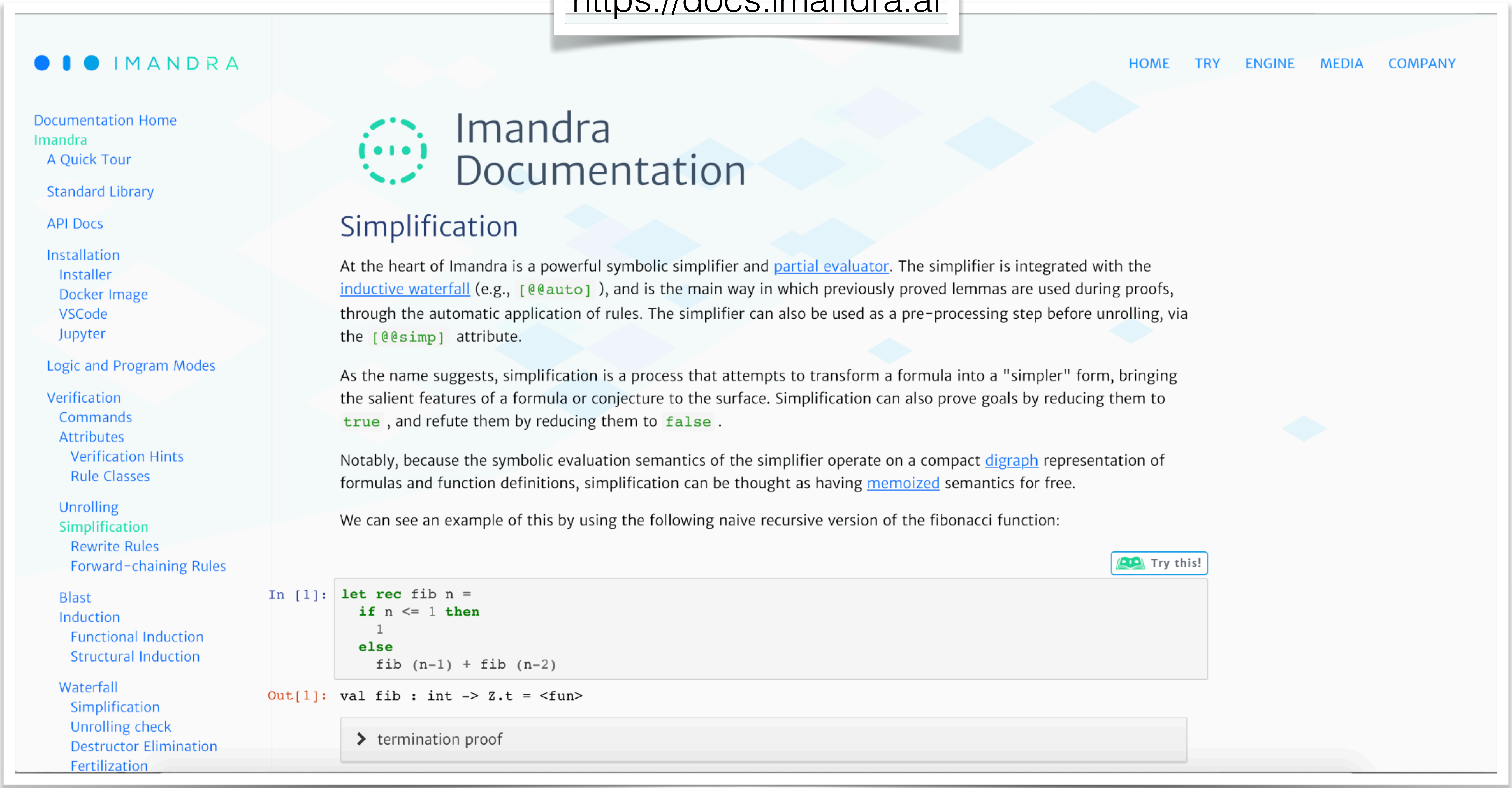


```
ai/imandra> #about

Imandra is:

- AI for algorithms, scaled to the cloud;
- a powerful new foundation for formally verified functional
programming;
- powering a new generation of tools for ensuring the safety,
fairness,  transparency and correctness of complex algorithms.

Imandra's Reasoning as a Service APIs democratise deep advances in
automated reasoning, bringing the power of tools traditionally
reserved for institutions like NASA to algorithm development at large.

Disclaimer: Imandra stores normalised representations of user
definitions, queries, counterexamples and proofs to improve future
performance.

Press here to consent and continue
```

You will find examples in finance, self-driving cars, robotics, hardware design, reinforcement learning and much more!

Extensive (interactive!) Online Documentation

https://docs.imandra.ai



Documentation Home
Imandra
- A Quick Tour
- Standard Library
- API Docs
- Installation
  - Installer
  - Docker Image
  - VSCode
  - Jupyter
- Logic and Program Modes
- Verification
  - Commands
  - Attributes
    - Verification Hints
    - Rule Classes
  - Unrolling
  - Simplification
    - Rewrite Rules
    - Forward-chaining Rules
  - Blast
  - Induction
    - Functional Induction
    - Structural Induction
  - Waterfall
    - Simplification
    - Unrolling check
    - Destructor Elimination
    - Fertilization

Imandra Documentation

Simplification

At the heart of Imandra is a powerful symbolic simplifier and partial evaluator. The simplifier is integrated with the inductive waterfall (e.g., `[@@auto]`), and is the main way in which previously proved lemmas are used during proofs, through the automatic application of rules. The simplifier can also be used as a pre-processing step before unrolling, via the `[@@simp]` attribute.

As the name suggests, simplification is a process that attempts to transform a formula into a "simpler" form, bringing the salient features of a formula or conjecture to the surface. Simplification can also prove goals by reducing them to `true` , and refute them by reducing them to `false` .

Notably, because the symbolic evaluation semantics of the simplifier operate on a compact digraph representation of formulas and function definitions, simplification can be thought as having memoized semantics for free.

We can see an example of this by using the following naive recursive version of the fibonacci function:

```
In [1]: let rec fib n =
          if n <= 1 then
            1
          else
            fib (n-1) + fib (n-2)

Out[1]: val fib : int -> Z.t = <fun>
```

> termination proof

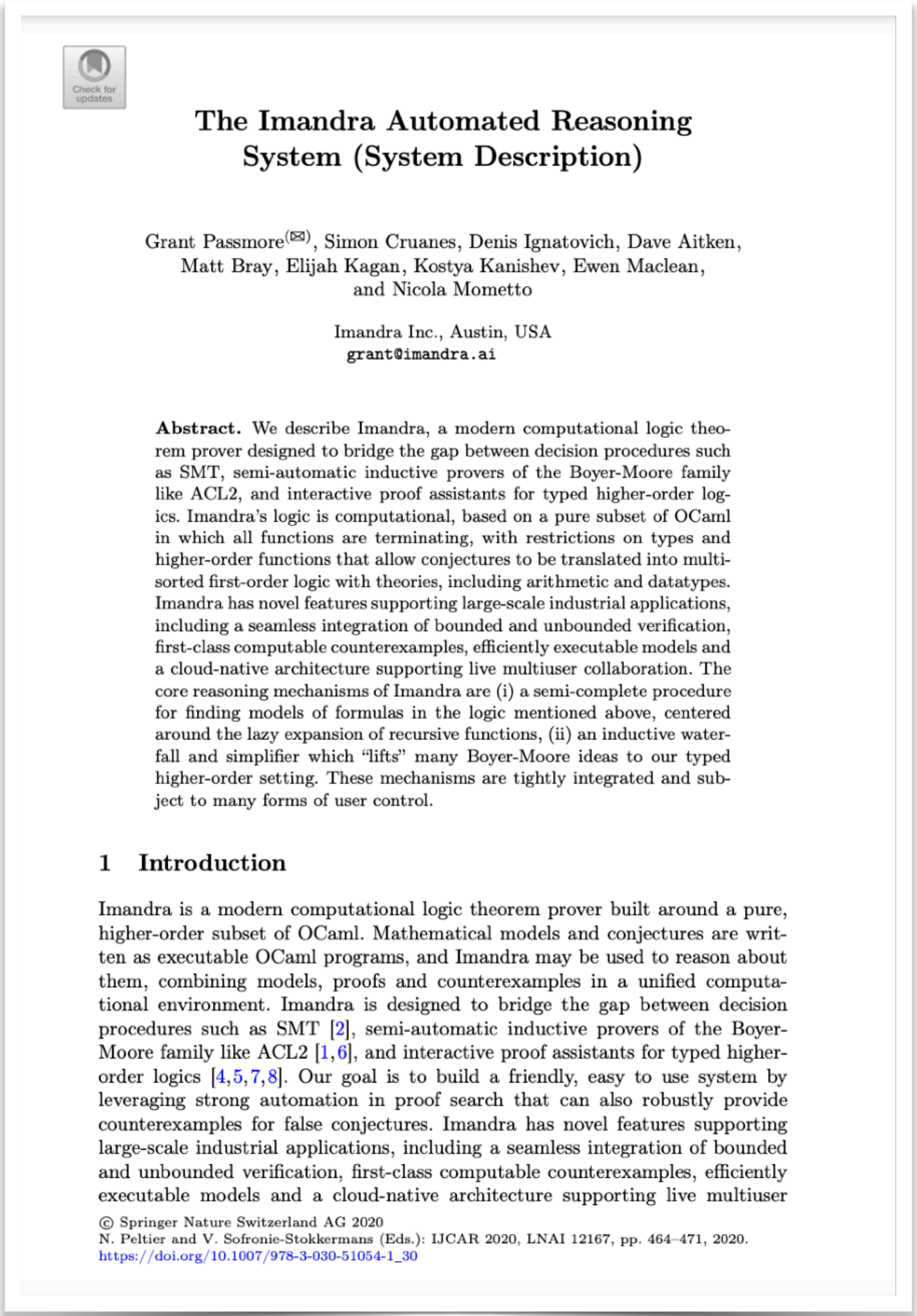
Big Ideas

OCaml + Automated Reasoning

- efficiently executable logic based on OCaml
- definitional principle based on ordinals (epsilon_0)
- first-class *(reflected)* computable counterexamples
- lifting of SMT to handle (higher-order, polymorphic) recursion and induction with Boyer-Moore-style waterfall (simplification, elimination, generalization, etc.)
- seamless integration of bounded and unbounded verification
- first-class notion of state-space decomposition
- cloud-native APIs, striving for tooling perfection :-)

IJCAR 2020

FM 2021



The Imandra Automated Reasoning System (System Description)

Grant Passmore(✉), Simon Cruanes, Denis Ignatovich, Dave Aitken,
Matt Bray, Elijah Kagan, Kostya Kanishev, Ewen Maclean,
and Nicola Mometto

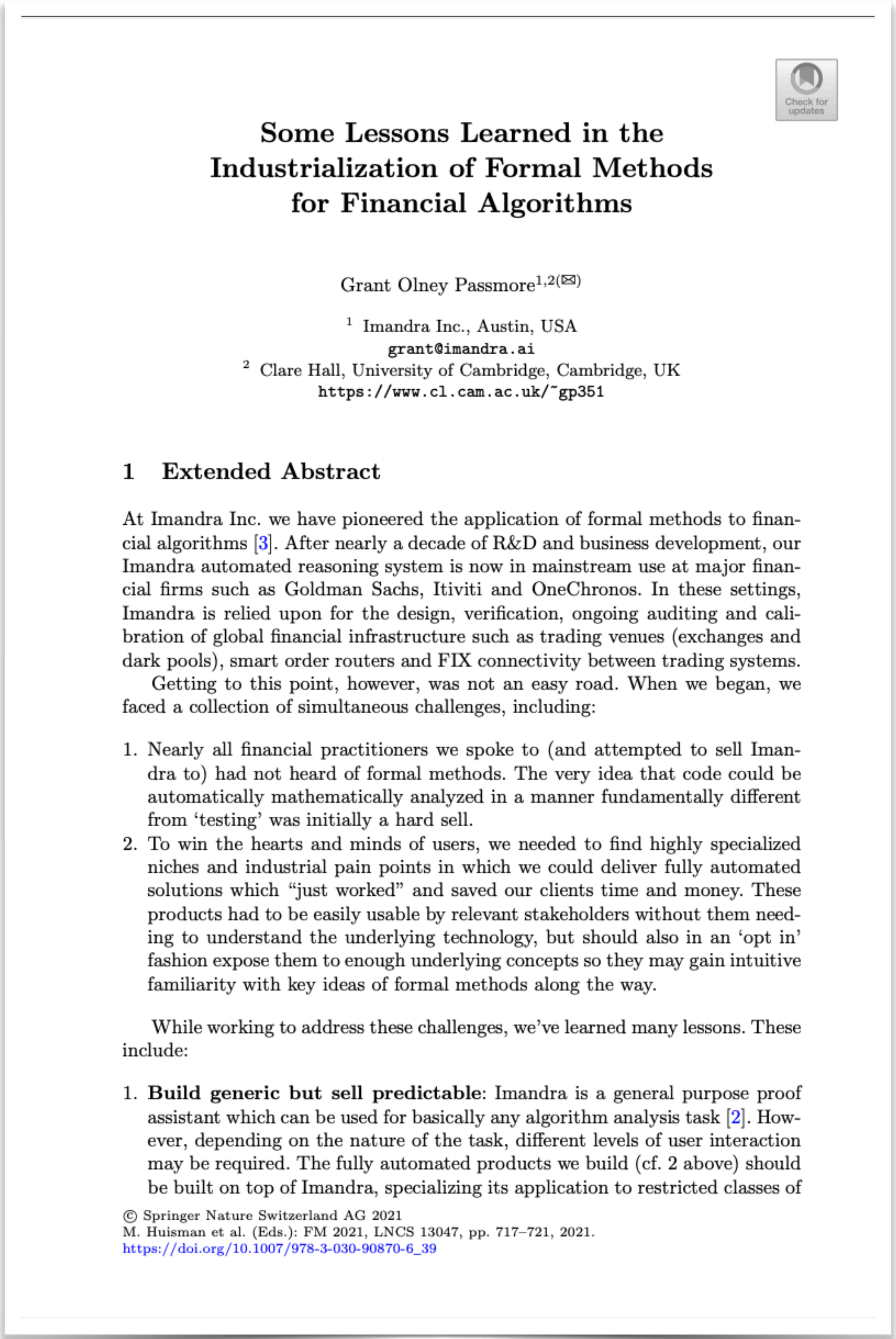
Imandra Inc., Austin, USA
grant@imandra.ai

Abstract. We describe Imandra, a modern computational logic theorem prover designed to bridge the gap between decision procedures such as SMT, semi-automatic inductive provers of the Boyer-Moore family like ACL2, and interactive proof assistants for typed higher-order logics. Imandra's logic is computational, based on a pure subset of OCaml in which all functions are terminating, with restrictions on types and higher-order functions that allow conjectures to be translated into multi-sorted first-order logic with theories, including arithmetic and datatypes. Imandra has novel features supporting large-scale industrial applications, including a seamless integration of bounded and unbounded verification, first-class computable counterexamples, efficiently executable models and a cloud-native architecture supporting live multiuser collaboration. The core reasoning mechanisms of Imandra are (i) a semi-complete procedure for finding models of formulas in the logic mentioned above, centered around the lazy expansion of recursive functions, (ii) an inductive waterfall and simplifier which "lifts" many Boyer-Moore ideas to our typed higher-order setting. These mechanisms are tightly integrated and subject to many forms of user control.

1 Introduction

Imandra is a modern computational logic theorem prover built around a pure, higher-order subset of OCaml. Mathematical models and conjectures are written as executable OCaml programs, and Imandra may be used to reason about them, combining models, proofs and counterexamples in a unified computational environment. Imandra is designed to bridge the gap between decision procedures such as SMT [2], semi-automatic inductive provers of the Boyer-Moore family like ACL2 [1,6], and interactive proof assistants for typed higher-order logics [4,5,7,8]. Our goal is to build a friendly, easy to use system by leveraging strong automation in proof search that can also robustly provide counterexamples for false conjectures. Imandra has novel features supporting large-scale industrial applications, including a seamless integration of bounded and unbounded verification, first-class computable counterexamples, efficiently executable models and a cloud-native architecture supporting live multiuser

© Springer Nature Switzerland AG 2020
N. Peltier and V. Sofronie-Stokkermans (Eds.): IJCAR 2020, LNAI 12167, pp. 464–471, 2020.
https://doi.org/10.1007/978-3-030-51054-1_30



Some Lessons Learned in the Industrialization of Formal Methods for Financial Algorithms

Grant Olney Passmore[1,2](✉)

[1] Imandra Inc., Austin, USA
grant@imandra.ai
[2] Clare Hall, University of Cambridge, Cambridge, UK
https://www.cl.cam.ac.uk/~gp351

1 Extended Abstract

At Imandra Inc. we have pioneered the application of formal methods to financial algorithms [3]. After nearly a decade of R&D and business development, our Imandra automated reasoning system is now in mainstream use at major financial firms such as Goldman Sachs, Itiviti and OneChronos. In these settings, Imandra is relied upon for the design, verification, ongoing auditing and calibration of global financial infrastructure such as trading venues (exchanges and dark pools), smart order routers and FIX connectivity between trading systems.

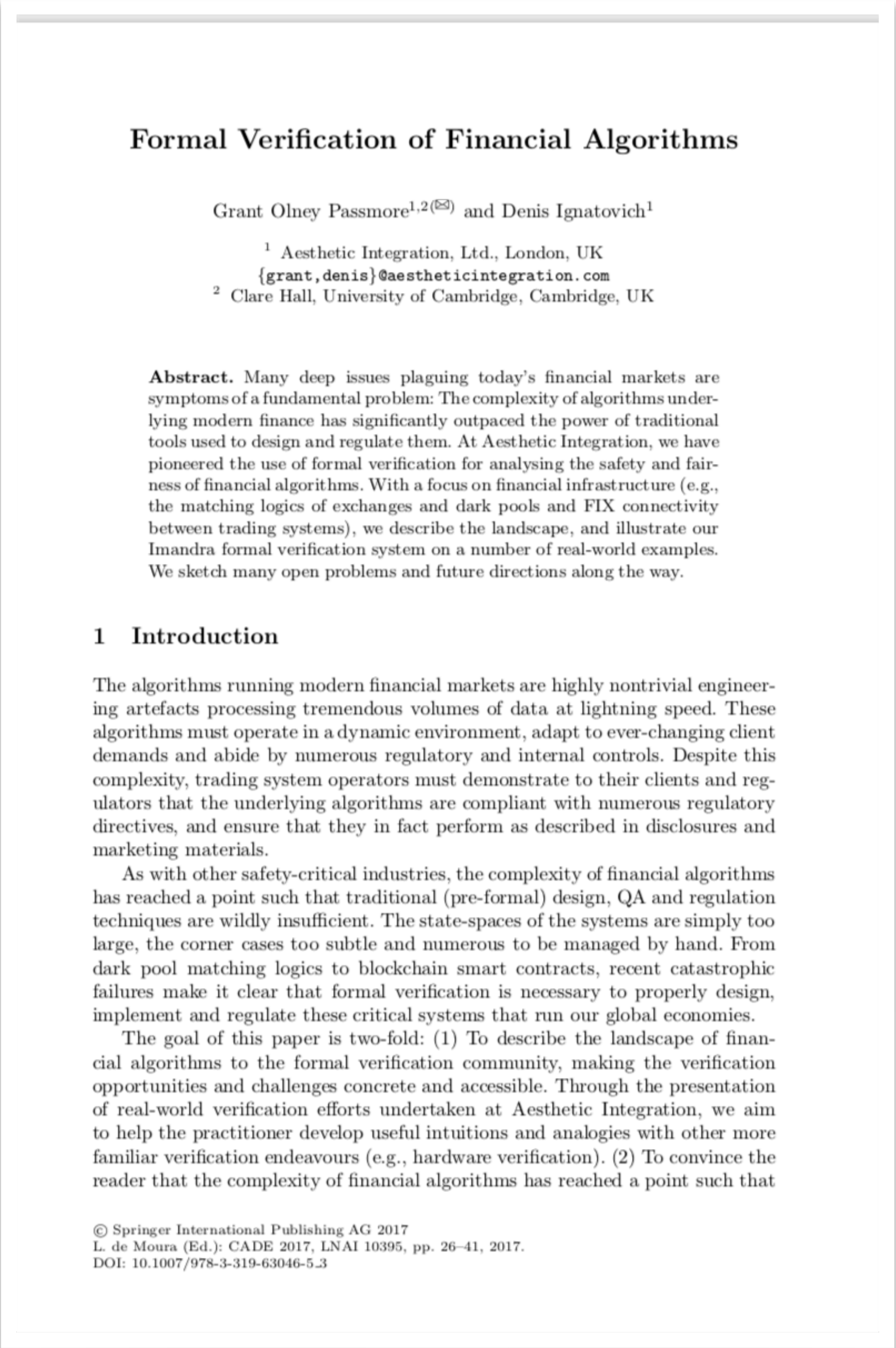
Getting to this point, however, was not an easy road. When we began, we faced a collection of simultaneous challenges, including:

1. Nearly all financial practitioners we spoke to (and attempted to sell Imandra to) had not heard of formal methods. The very idea that code could be automatically mathematically analyzed in a manner fundamentally different from 'testing' was initially a hard sell.
2. To win the hearts and minds of users, we needed to find highly specialized niches and industrial pain points in which we could deliver fully automated solutions which "just worked" and saved our clients time and money. These products had to be easily usable by relevant stakeholders without them needing to understand the underlying technology, but should also in an 'opt in' fashion expose them to enough underlying concepts so they may gain intuitive familiarity with key ideas of formal methods along the way.

While working to address these challenges, we've learned many lessons. These include:

1. **Build generic but sell predictable**: Imandra is a general purpose proof assistant which can be used for basically any algorithm analysis task [2]. However, depending on the nature of the task, different levels of user interaction may be required. The fully automated products we build (cf. 2 above) should be built on top of Imandra, specializing its application to restricted classes of

© Springer Nature Switzerland AG 2021
M. Huisman et al. (Eds.): FM 2021, LNCS 13047, pp. 717–721, 2021.
https://doi.org/10.1007/978-3-030-90870-6_39



Formal Verification of Financial Algorithms

Grant Olney Passmore[1,2](✉) and Denis Ignatovich[1]

[1] Aesthetic Integration, Ltd., London, UK
{grant,denis}@aestheticintegration.com
[2] Clare Hall, University of Cambridge, Cambridge, UK

Abstract. Many deep issues plaguing today's financial markets are symptoms of a fundamental problem: The complexity of algorithms underlying modern finance has significantly outpaced the power of traditional tools used to design and regulate them. At Aesthetic Integration, we have pioneered the use of formal verification for analysing the safety and fairness of financial algorithms. With a focus on financial infrastructure (e.g., the matching logics of exchanges and dark pools and FIX connectivity between trading systems), we describe the landscape, and illustrate our Imandra formal verification system on a number of real-world examples. We sketch many open problems and future directions along the way.

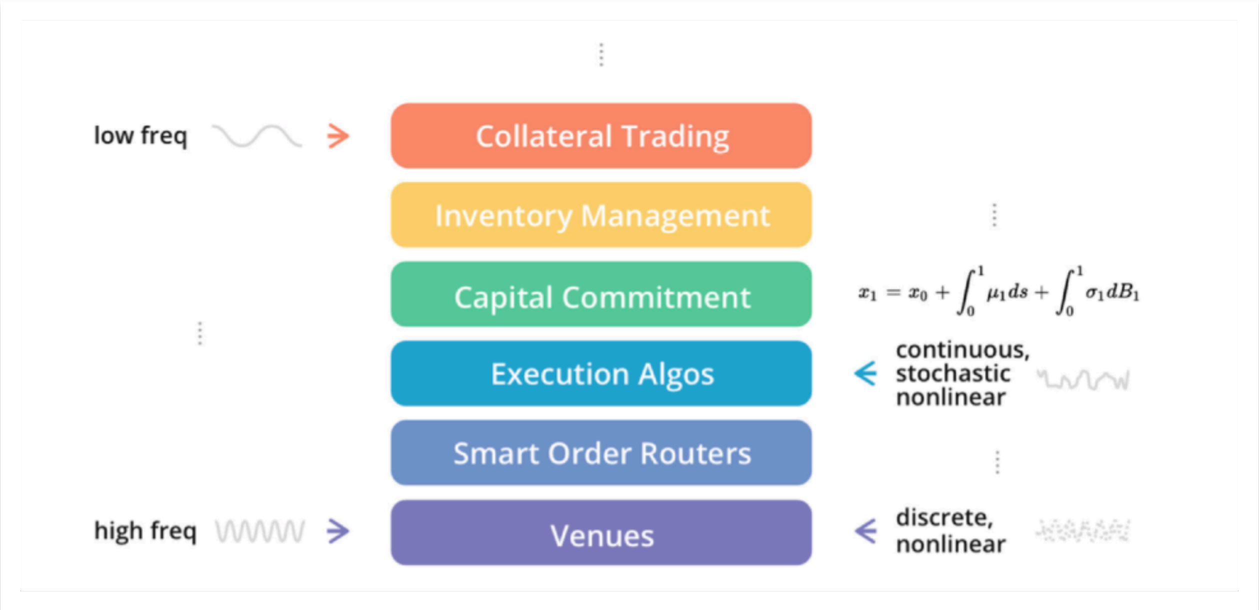
1 Introduction

The algorithms running modern financial markets are highly nontrivial engineering artefacts processing tremendous volumes of data at lightning speed. These algorithms must operate in a dynamic environment, adapt to ever-changing client demands and abide by numerous regulatory and internal controls. Despite this complexity, trading system operators must demonstrate to their clients and regulators that the underlying algorithms are compliant with numerous regulatory directives, and ensure that they in fact perform as described in disclosures and marketing materials.

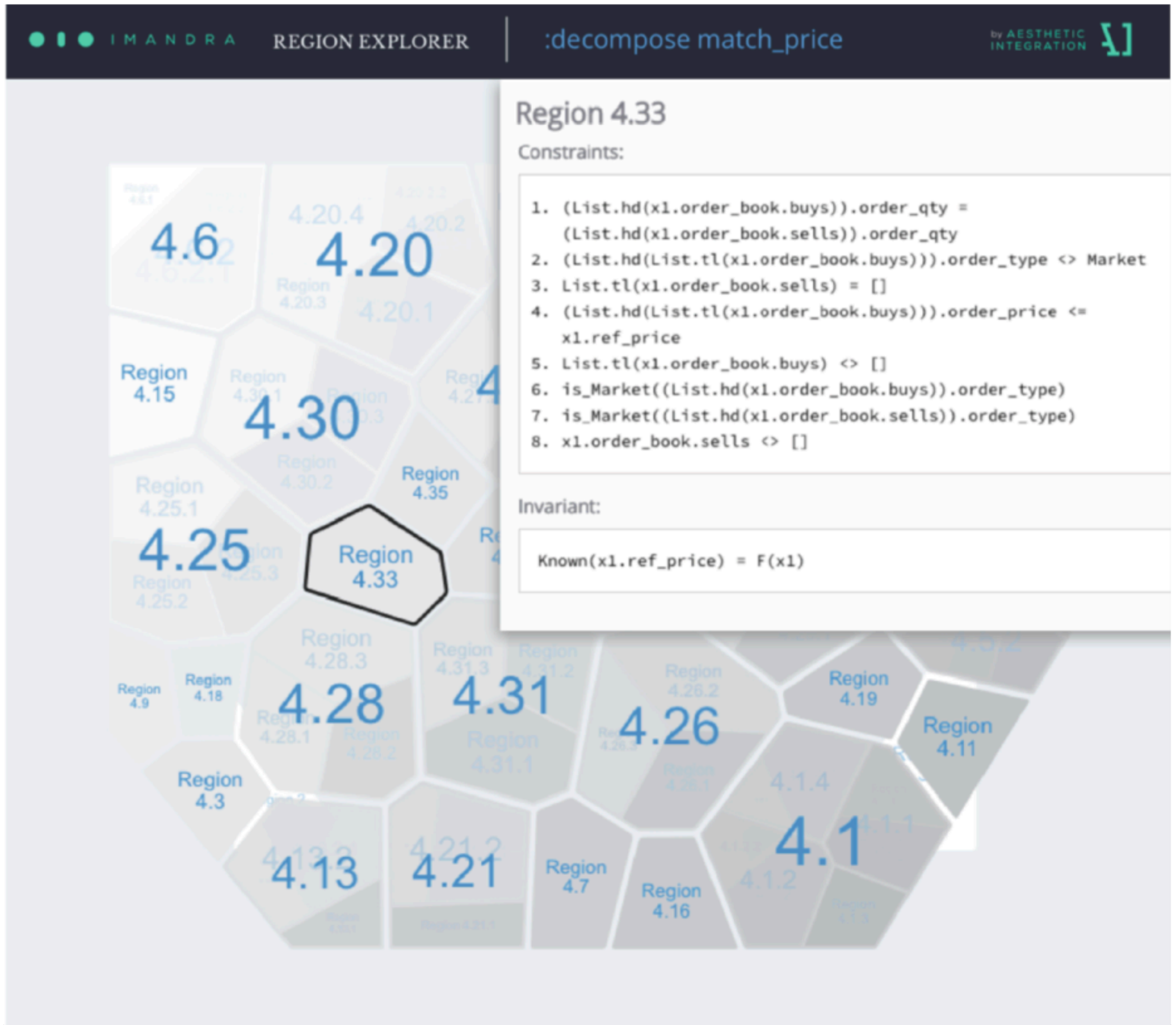
As with other safety-critical industries, the complexity of financial algorithms has reached a point such that traditional (pre-formal) design, QA and regulation techniques are wildly insufficient. The state-spaces of the systems are simply too large, the corner cases too subtle and numerous to be managed by hand. From dark pool matching logics to blockchain smart contracts, recent catastrophic failures make it clear that formal verification is necessary to properly design, implement and regulate these critical systems that run our global economies.

The goal of this paper is two-fold: (1) To describe the landscape of financial algorithms to the formal verification community, making the verification opportunities and challenges concrete and accessible. Through the presentation of real-world verification efforts undertaken at Aesthetic Integration, we aim to help the practitioner develop useful intuitions and analogies with other more familiar verification endeavours (e.g., hardware verification). (2) To convince the reader that the complexity of financial algorithms has reached a point such that

L. de Moura (Ed.): CADE 2017, LNAI 10395, pp. 26–41, 2017.
DOI: 10.1007/978-3-319-63046-5_3



$$x_1 = x_0 + \int_0^1 \mu_1 ds + \int_0^1 \sigma_1 dB_1$$



Region 4.33

Constraints:

```
1. (List.hd(x1.order_book.buys)).order_qty =
   (List.hd(x1.order_book.sells)).order_qty
2. (List.hd(List.tl(x1.order_book.buys))).order_type <> Market
3. List.tl(x1.order_book.sells) = []
4. (List.hd(List.tl(x1.order_book.buys))).order_price <=
   x1.ref_price
5. List.tl(x1.order_book.buys) <> []
6. is_Market((List.hd(x1.order_book.buys)).order_type)
7. is_Market((List.hd(x1.order_book.sells)).order_type)
8. x1.order_book.sells <> []
```

Invariant:

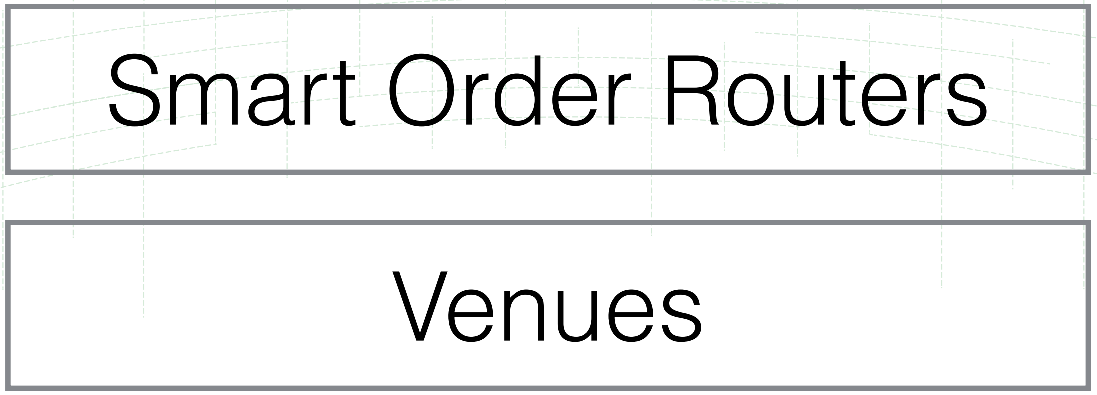
```
Known(x1.ref_price) = F(x1)
```

The Stack of Financial Algorithms

The Stack of Financial Algorithms

Venues

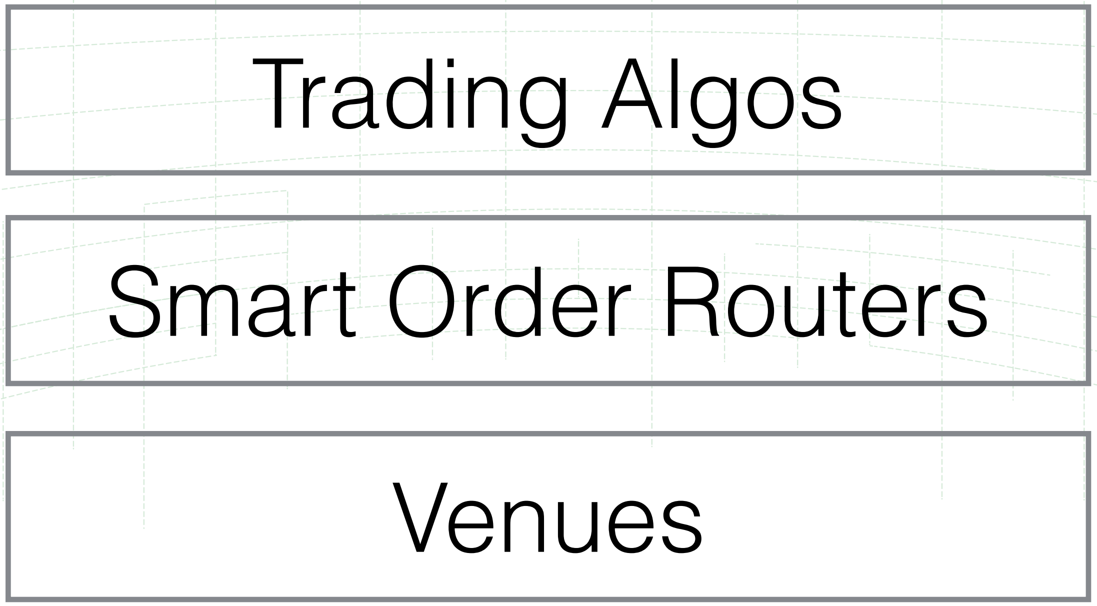
The Stack of Financial Algorithms



Smart Order Routers

Venues

The Stack of Financial Algorithms

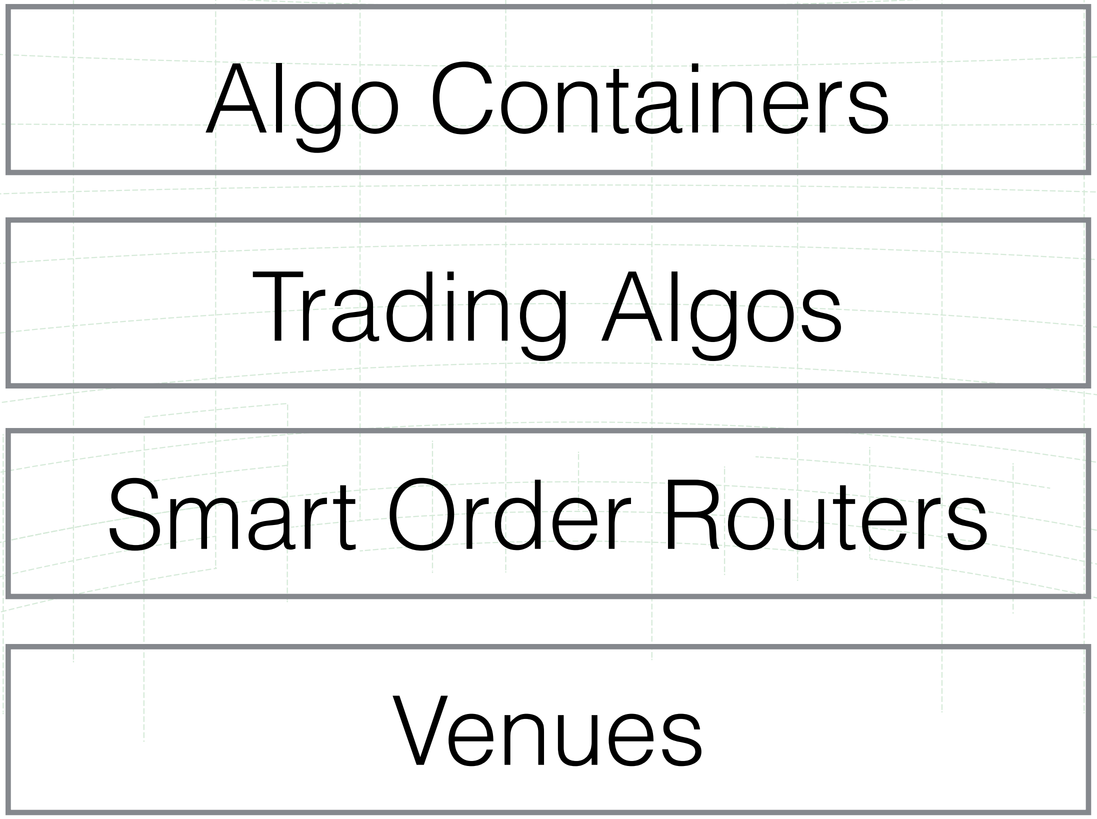


Trading Algos

Smart Order Routers

Venues

The Stack of Financial Algorithms



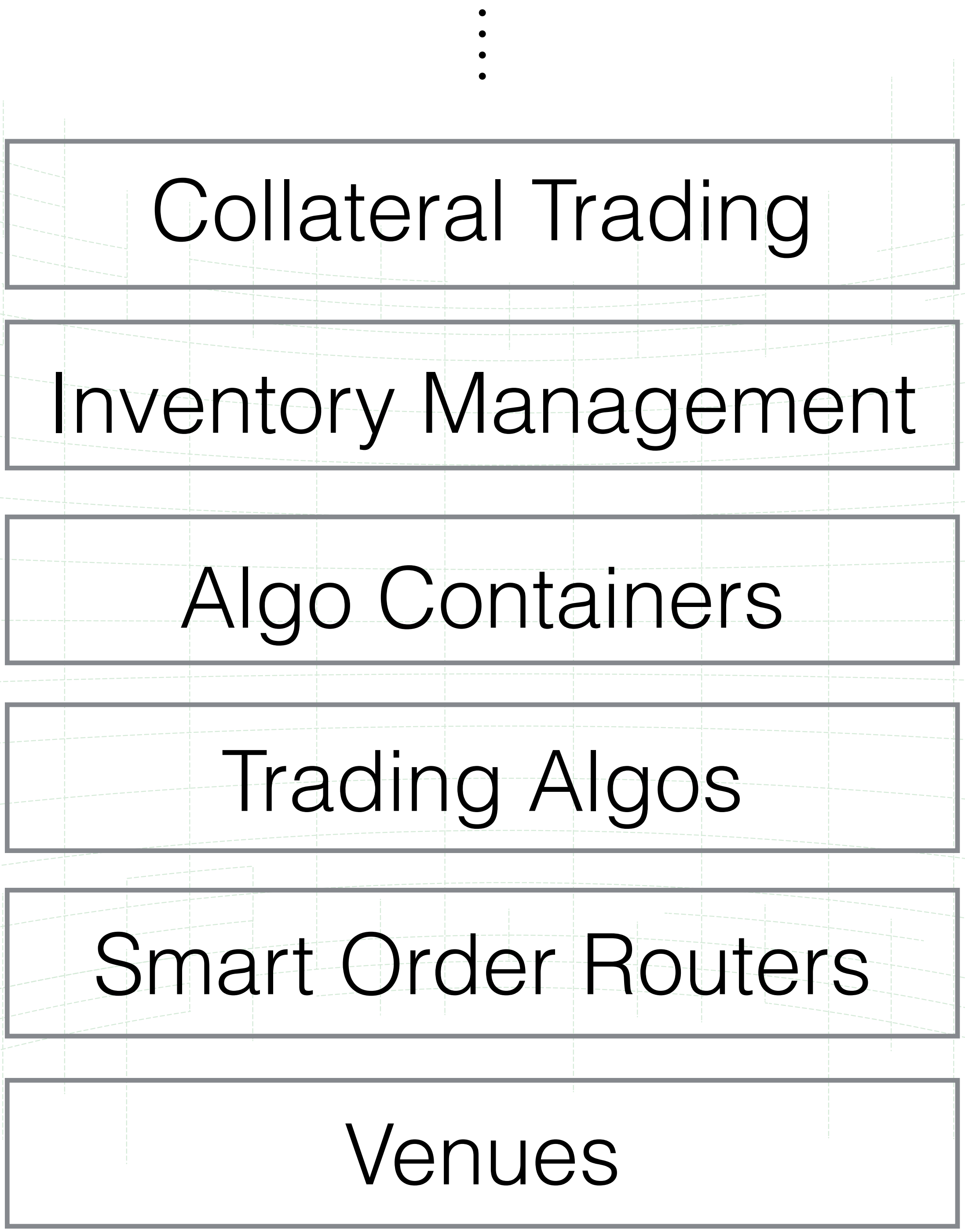
Algo Containers

Trading Algos

Smart Order Routers

Venues

The Stack of Financial Algorithms



⋮

Collateral Trading

Inventory Management

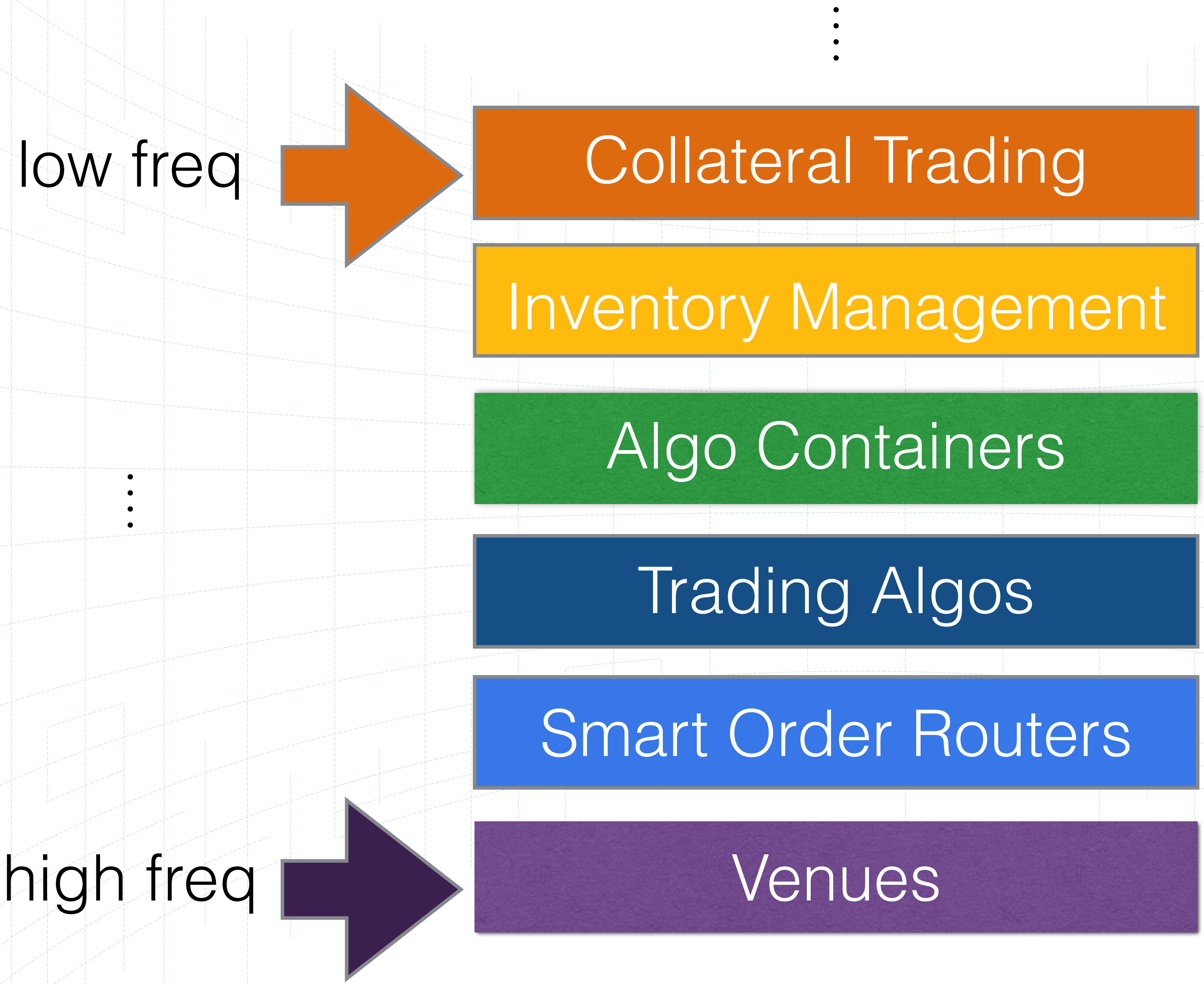
Algo Containers

Trading Algos

Smart Order Routers

Venues

The Stack of Financial Algorithms



⋮

low freq

Collateral Trading

Inventory Management

Algo Containers

⋮

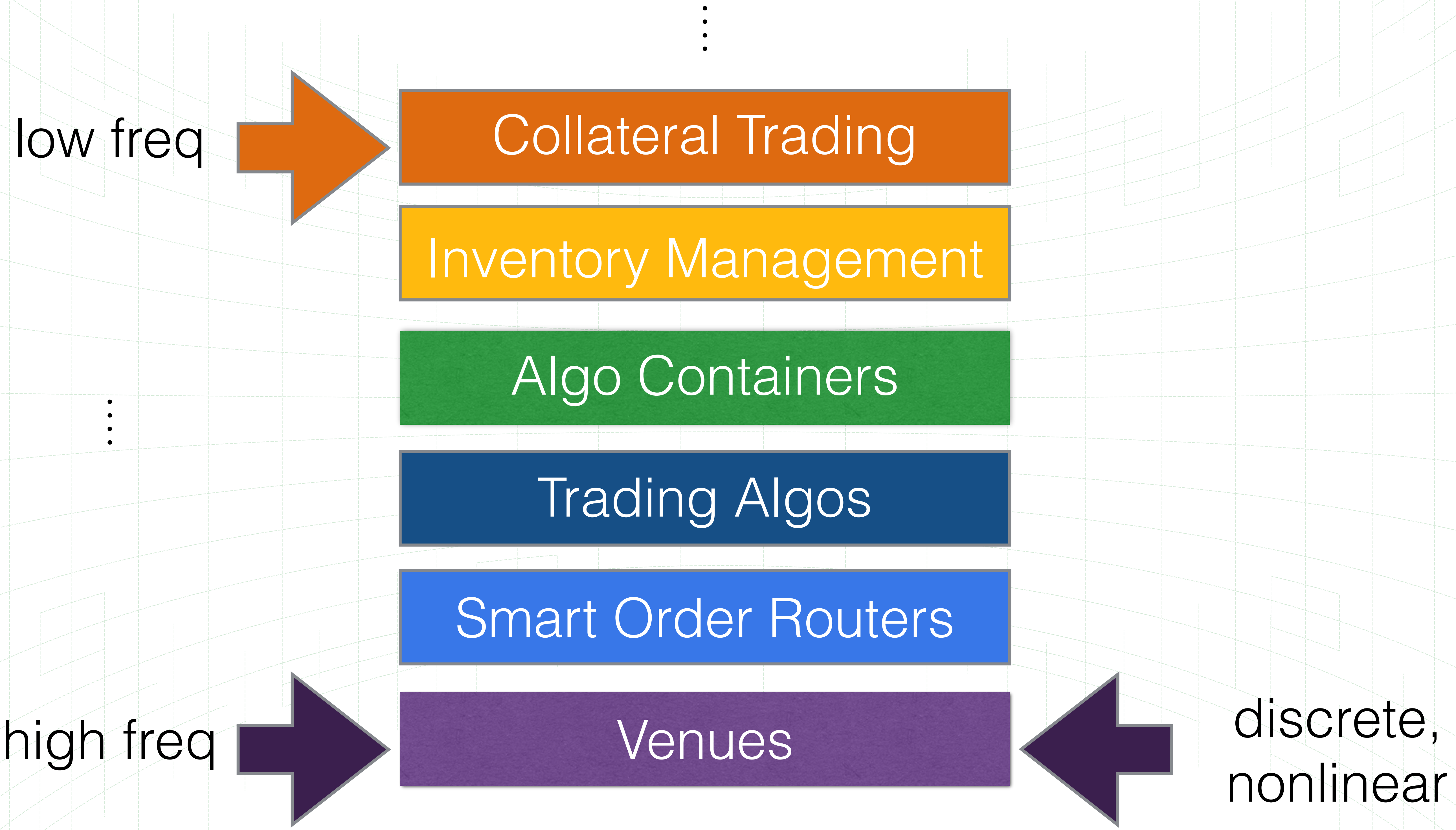
Trading Algos

Smart Order Routers

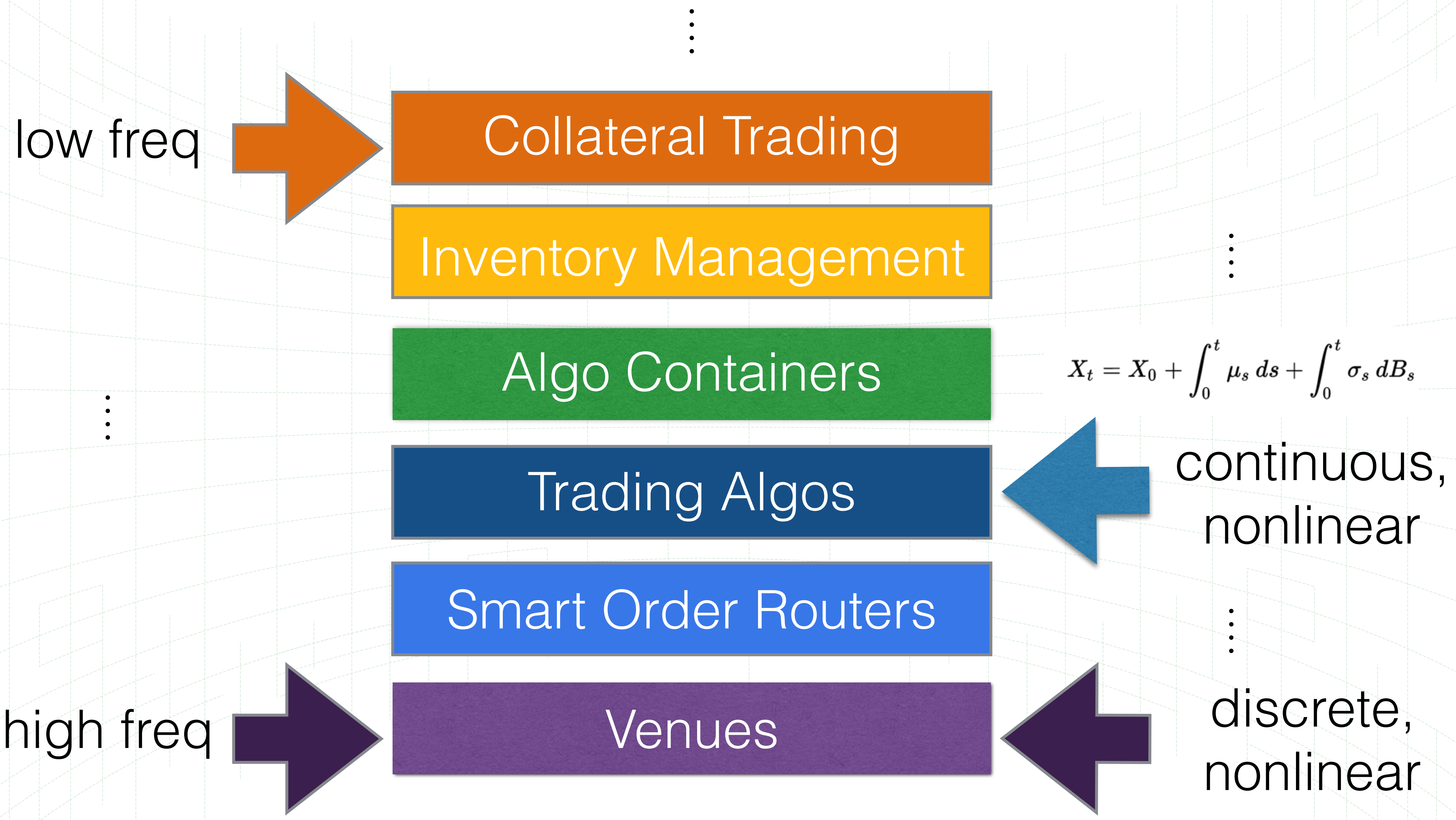
high freq

Venues

The Stack of Financial Algorithms



The Stack of Financial Algorithms



⋮

low freq

Collateral Trading

Inventory Management

Algo Containers

Trading Algos

Smart Order Routers

Venues

high freq

⋮

$$X_t = X_0 + \int_0^t \mu_s \, ds + \int_0^t \sigma_s \, dB_s$$

continuous, nonlinear

⋮

discrete, nonlinear

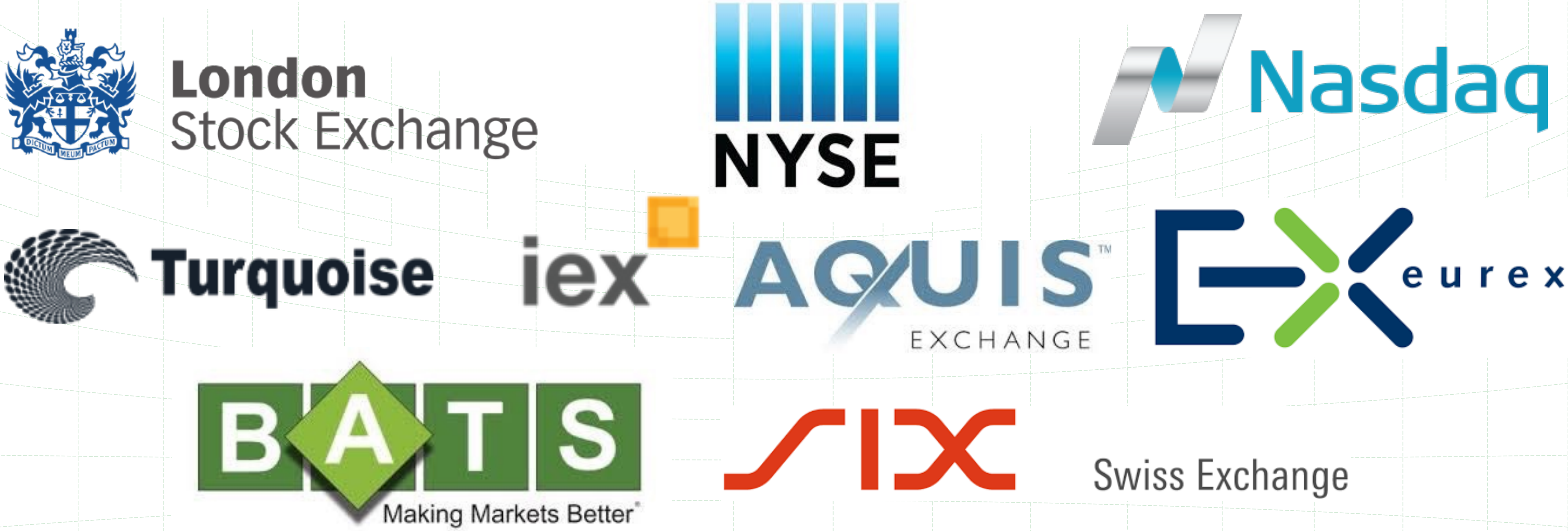
What is a venue?

London
Stock Exchange

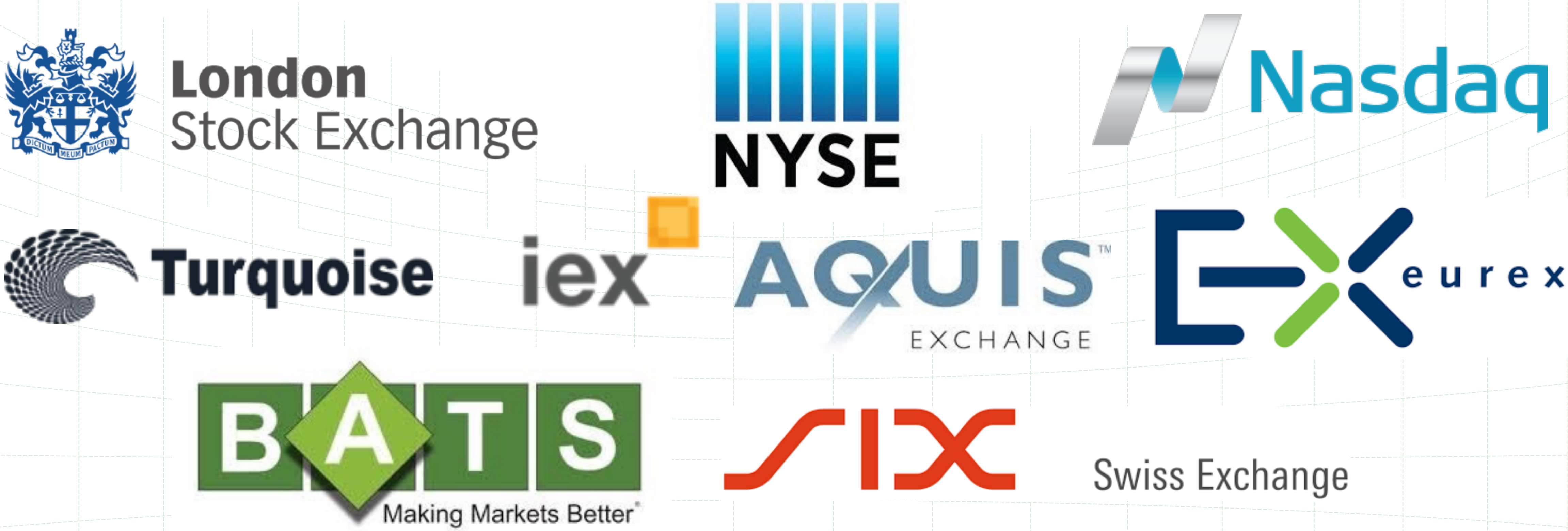
NYSE

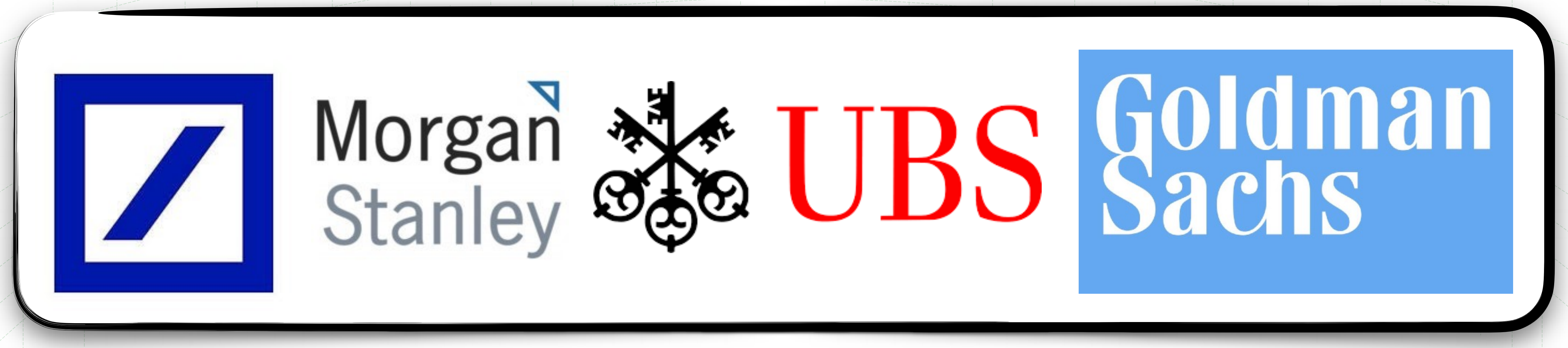
Nasdaq

What is a venue?



What is a venue?





What is a venue?

London Stock Exchange
NYSE
Nasdaq
Turquoise
iex
AQUIS EXCHANGE
eurex
BATS
Making Markets Better
SIX
Swiss Exchange

LIT LIQUIDITY

Morgan Stanley
UBS
Goldman Sachs

DARK LIQUIDITY

What is an order type?

MARKET ORDER

What is an order type?

MARKET ORDER

LIMIT ORDER

What is an order type?

MARKET ORDER

LIMIT ORDER

ICEBERG ORDER

What is an order type?

MARKET ORDER

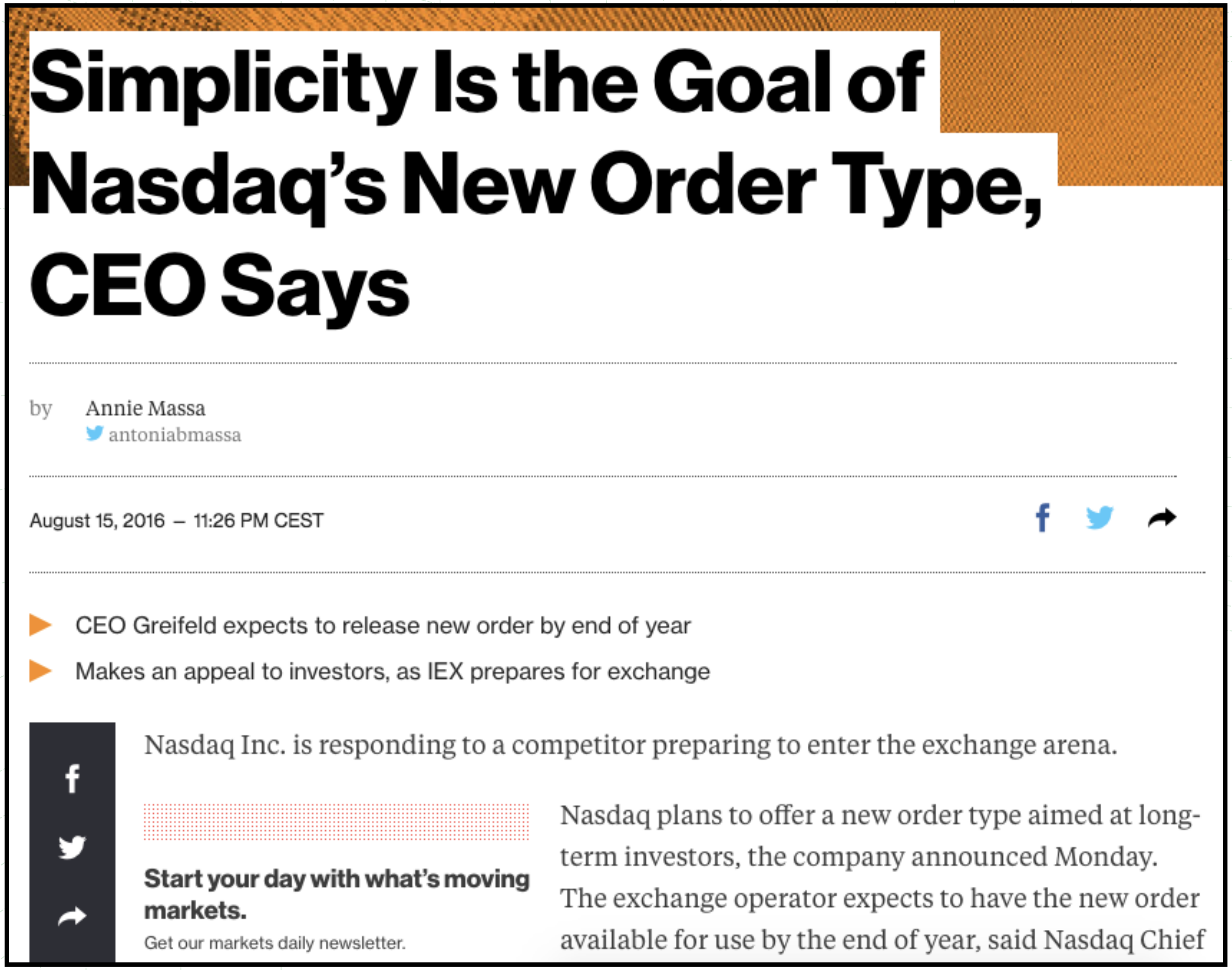
LIMIT ORDER

ICEBERG ORDER

STOP LOSS ORDER

⋮

What is an order type?



Simplicity Is the Goal of Nasdaq's New Order Type, CEO Says

by Annie Massa
antoniabmassa

August 15, 2016 – 11:26 PM CEST

- CEO Greifeld expects to release new order by end of year
- Makes an appeal to investors, as IEX prepares for exchange

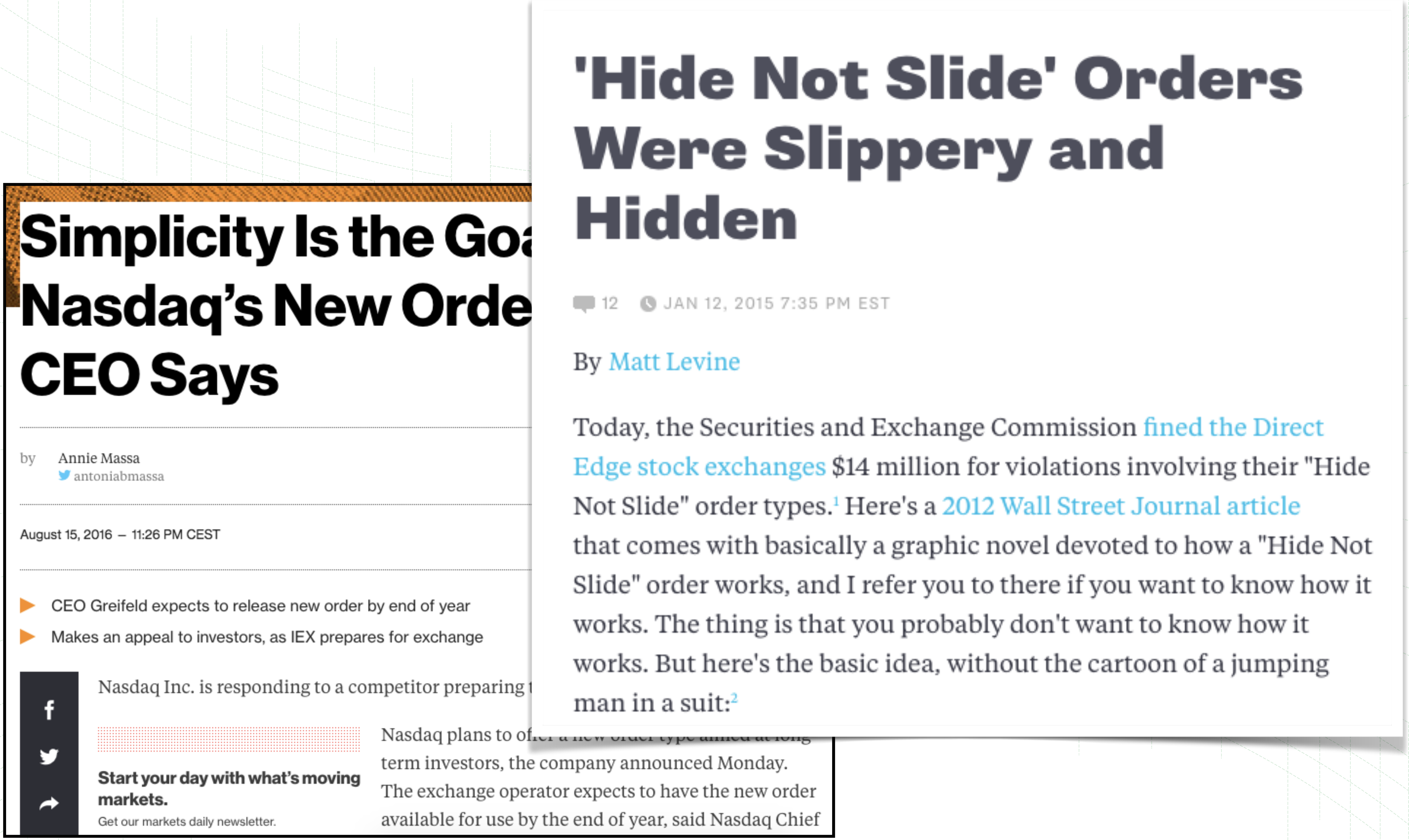
Nasdaq Inc. is responding to a competitor preparing to enter the exchange arena.

Start your day with what's moving markets.

Get our markets daily newsletter.

Nasdaq plans to offer a new order type aimed at long-term investors, the company announced Monday. The exchange operator expects to have the new order available for use by the end of year, said Nasdaq Chief

What is an order type?



Simplicity Is the Goa Nasdaq's New Orde CEO Says

by Annie Massa
antoniabmassa

August 15, 2016 – 11:26 PM CEST

- CEO Greifeld expects to release new order by end of year
- Makes an appeal to investors, as IEX prepares for exchange

Nasdaq Inc. is responding to a competitor preparing t

Start your day with what's moving markets.

Get our markets daily newsletter.

Nasdaq plans to of term investors, the company announced Monday. The exchange operator expects to have the new order available for use by the end of year, said Nasdaq Chief

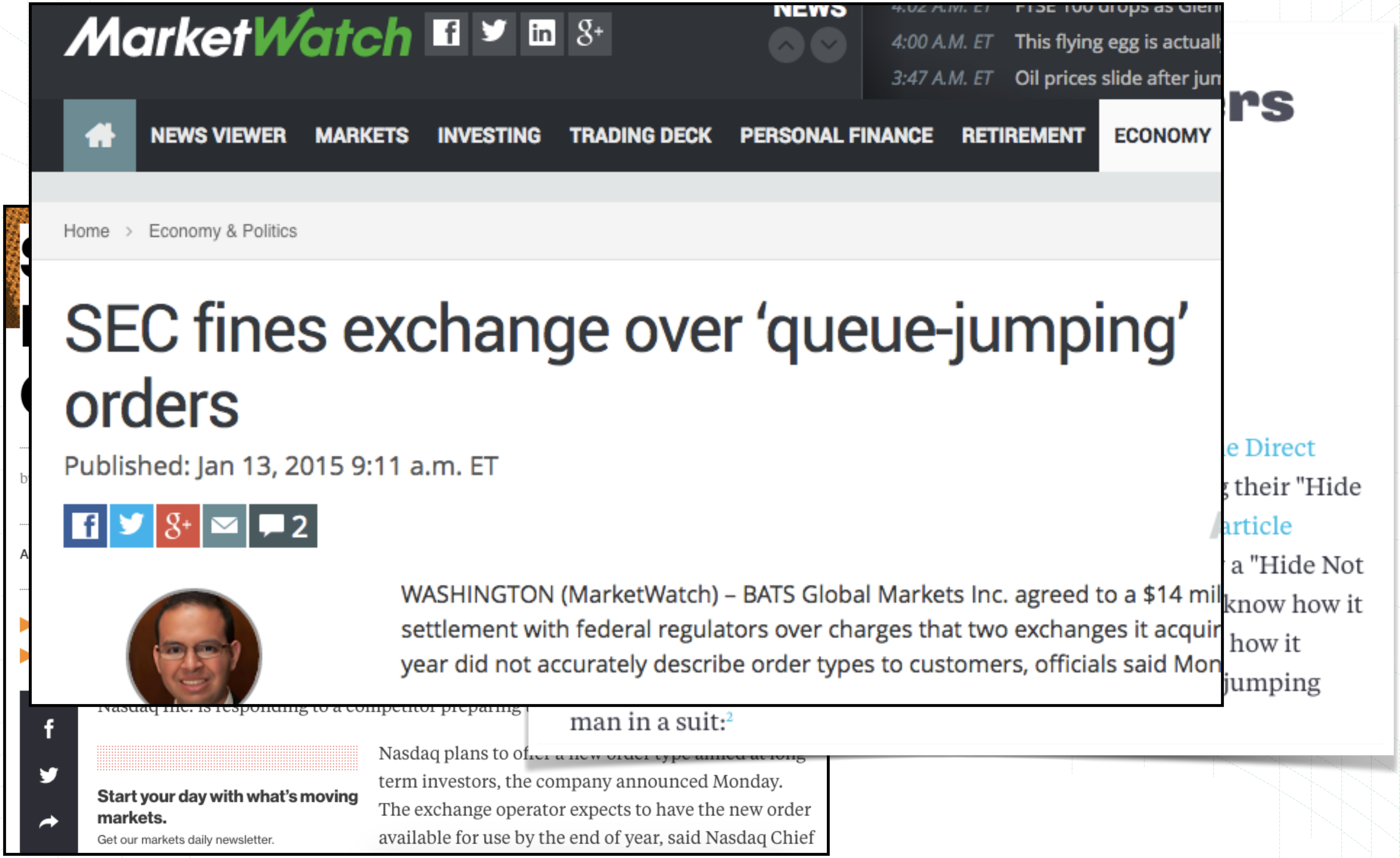
'Hide Not Slide' Orders Were Slippery and Hidden

12 JAN 12, 2015 7:35 PM EST

By Matt Levine

Today, the Securities and Exchange Commission fined the Direct Edge stock exchanges $14 million for violations involving their "Hide Not Slide" order types.[1] Here's a 2012 Wall Street Journal article that comes with basically a graphic novel devoted to how a "Hide Not Slide" order works, and I refer you to there if you want to know how it works. The thing is that you probably don't want to know how it works. But here's the basic idea, without the cartoon of a jumping man in a suit:[2]

What is an order type?



MarketWatch

NEWS

4:02 A.M. ET FTSE 100 drops as Glen

4:00 A.M. ET This flying egg is actuall

3:47 A.M. ET Oil prices slide after jun

Home > Economy & Politics

SEC fines exchange over 'queue-jumping' orders

Published: Jan 13, 2015 9:11 a.m. ET

2

WASHINGTON (MarketWatch) – BATS Global Markets Inc. agreed to a $14 mil settlement with federal regulators over charges that two exchanges it acquir year did not accurately describe order types to customers, officials said Mon

rs

e Direct

their "Hide

article

a "Hide Not

know how it

how it

jumping

man in a suit:[2]

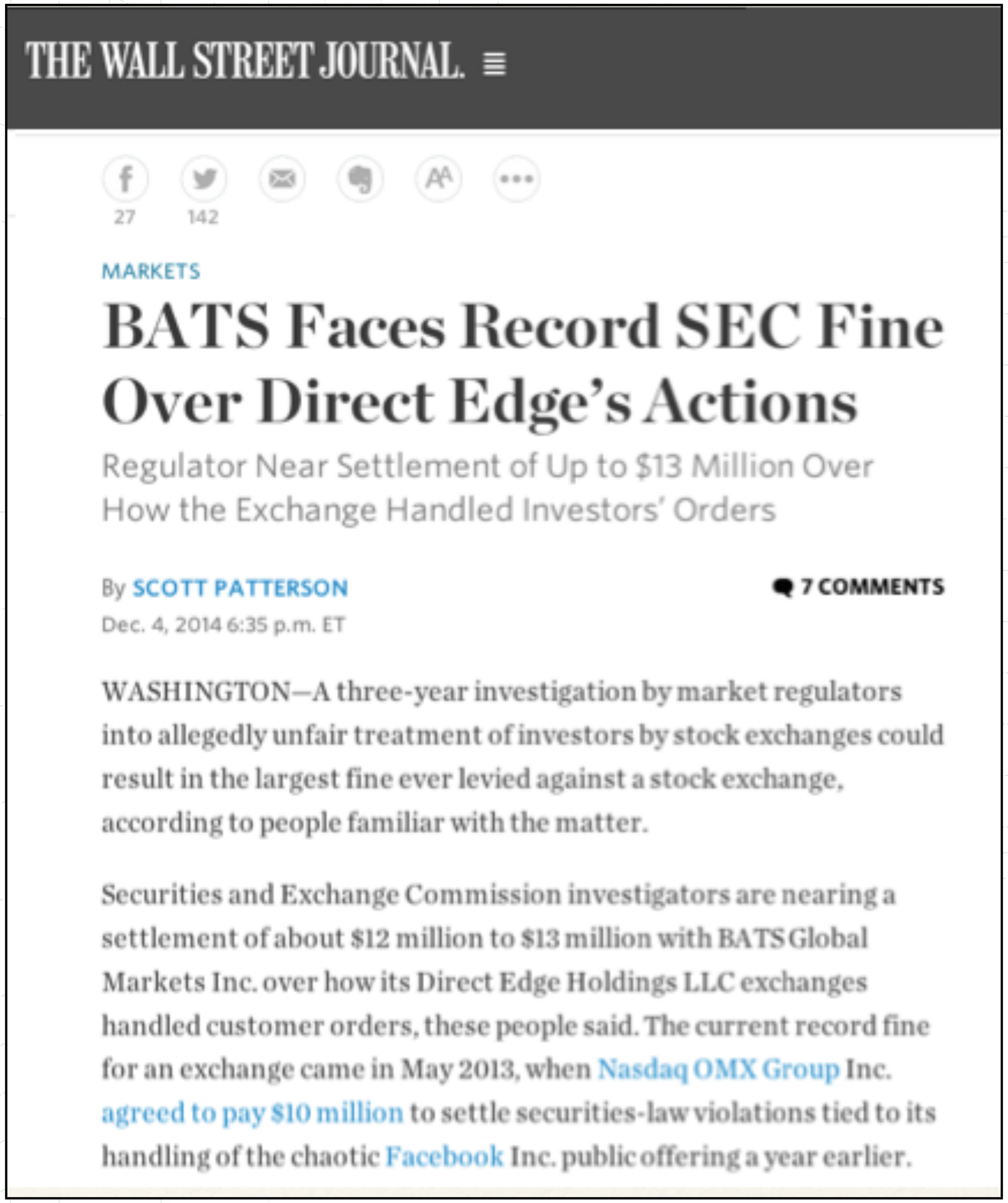
Nasdaq Inc. is responding to a competitor preparing

Start your day with what's moving markets.

Get our markets daily newsletter.

Nasdaq plans to offer a new order type aimed at long term investors, the company announced Monday. The exchange operator expects to have the new order available for use by the end of year, said Nasdaq Chief

Is your venue fair?



MARKETS

BATS Faces Record SEC Fine Over Direct Edge's Actions

Regulator Near Settlement of Up to $13 Million Over How the Exchange Handled Investors' Orders

By SCOTT PATTERSON

7 COMMENTS

Dec. 4, 2014 6:35 p.m. ET

WASHINGTON—A three-year investigation by market regulators into allegedly unfair treatment of investors by stock exchanges could result in the largest fine ever levied against a stock exchange, according to people familiar with the matter.

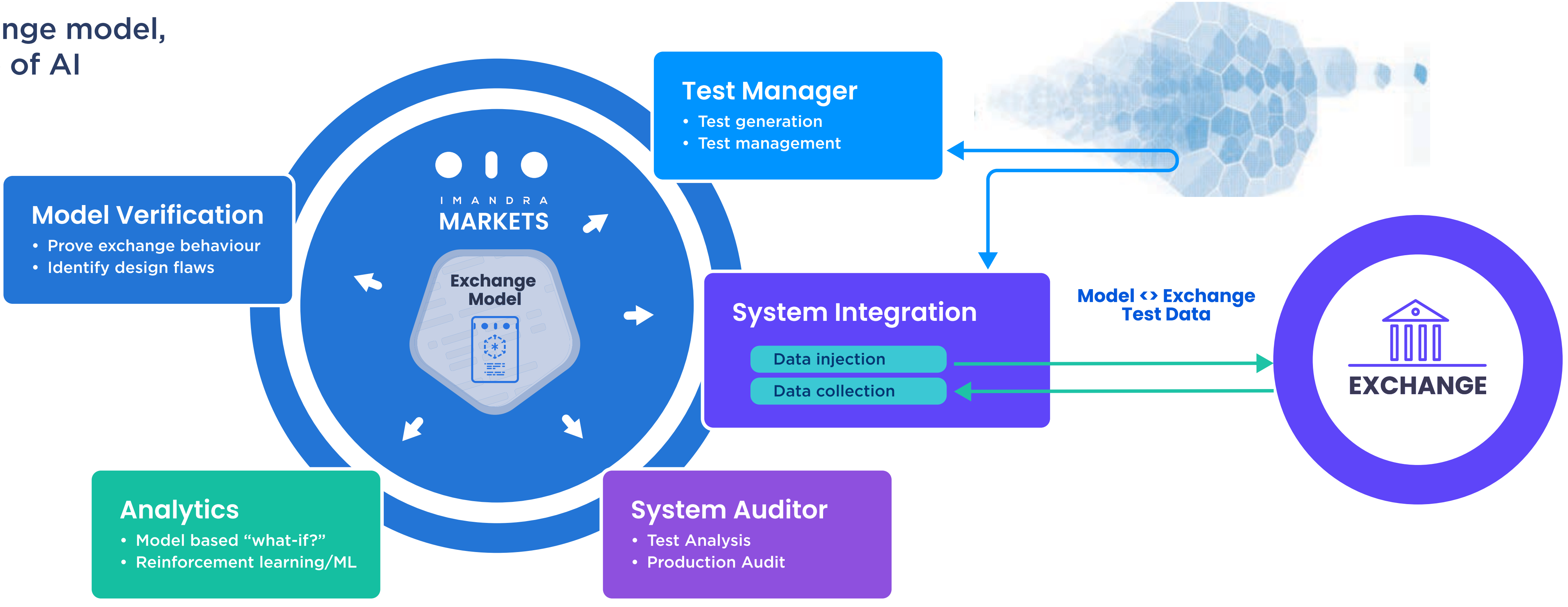
Securities and Exchange Commission investigators are nearing a settlement of about $12 million to $13 million with BATS Global Markets Inc. over how its Direct Edge Holdings LLC exchanges handled customer orders, these people said. The current record fine for an exchange came in May 2013, when Nasdaq OMX Group Inc. agreed to pay $10 million to settle securities-law violations tied to its handling of the chaotic Facebook Inc. public offering a year earlier.

Difficult questions:

- Is your venue *fair*?
- Can you *prove* it?
- If it's not fair, how can you *fix* it?
- Can your collection of order-types ever *violate* regulatory directives?
- Does your high-performance *implementation* conform to your high-level design specification?
- Does your *documentation* of your order-types truly match your implementation?
- How can you *automate* both *testing* and *compliance*?
- What is the *strongest possible evidence* you can give to regulators?

Imandra Markets

Centred around the exchange model, Imandra Markets is a suite of AI powered services.



Test Manager

- Test generation
- Test management

Model Verification

- Prove exchange behaviour
- Identify design flaws

System Integration

- Data injection
- Data collection

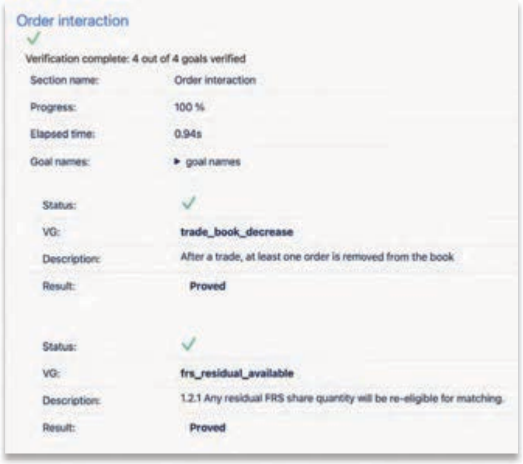
Analytics

- Model based “what-if?”
- Reinforcement learning/ML

System Auditor

- Test Analysis
- Production Audit

Formally verified key regulatory properties



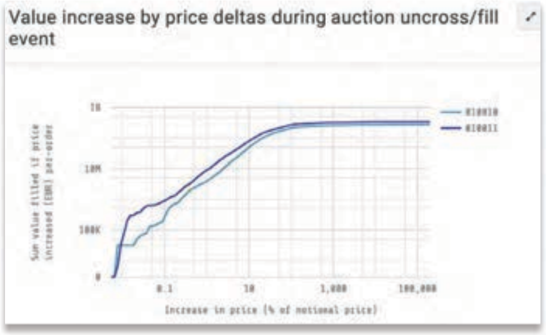
Order interaction

✓

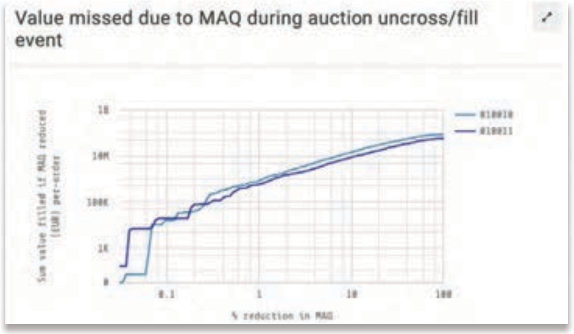
Verification complete: 4 out of 4 goals verified

Section name:	Order interaction
Progress:	100 %
Elapsed time:	0.94s
Goal names:	▸ goal names
Status:	✓
VG:	**trade_book_decrease**
Description:	After a trade, at least one order is removed from the book
Result:	**Proved**
Status:	✓
VG:	**frs_residual_available**
Description:	1.2.1 Any residual FRS share quantity will be re-eligible for matching.
Result:	**Proved**

Venue Insights - Business Intelligence

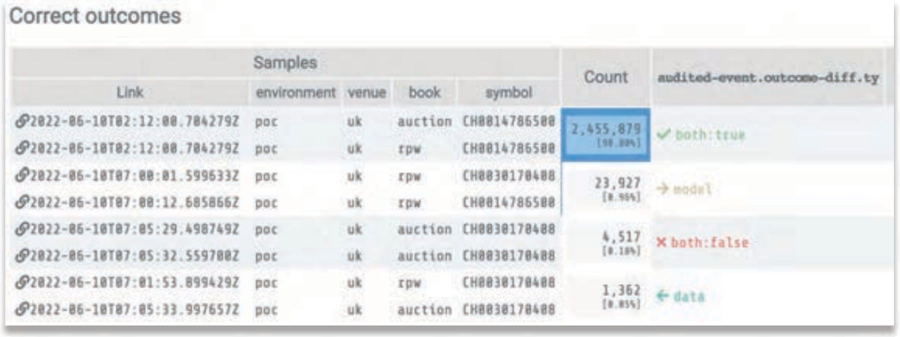


Value increase by price deltas during auction uncross/fill event



Value missed due to MAQ during auction uncross/fill event

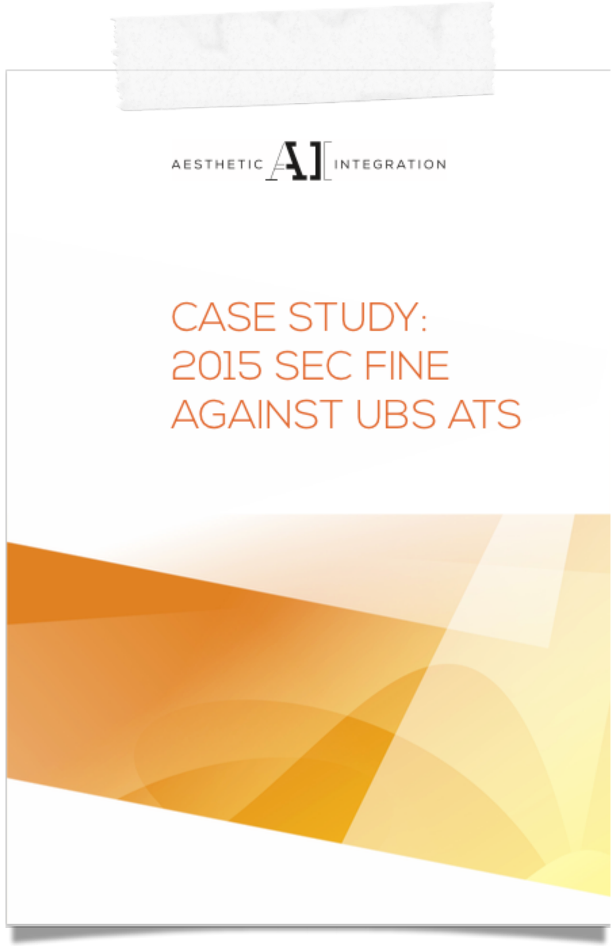
Production Data Audit



Correct outcomes

Samples					Count	audited-event.outcome-diff.ty
Link	environment	venue	book	symbol		
2022-06-10T02:12:00.704279Z	poc	uk	auction	CH0014786500	2,455,879 [98.80%]	✓ both:true
2022-06-10T02:12:00.704279Z	poc	uk	rpw	CH0014786500		
2022-06-10T07:00:01.599633Z	poc	uk	rpw	CH0030170408	23,927 [0.96%]	→ model
2022-06-10T07:00:12.685866Z	poc	uk	rpw	CH0014786500		
2022-06-10T07:05:29.498749Z	poc	uk	auction	CH0030170408	4,517 [0.18%]	✗ both:false
2022-06-10T07:05:32.559700Z	poc	uk	auction	CH0030170408		
2022-06-10T07:01:53.899429Z	poc	uk	rpw	CH0030170408	1,362 [0.05%]	← data
2022-06-10T07:05:33.997657Z	poc	uk	auction	CH0030170408		

Case Study: UBS ATS



AESTHETIC AI INTEGRATION

CASE STUDY:
2015 SEC FINE
AGAINST UBS ATS

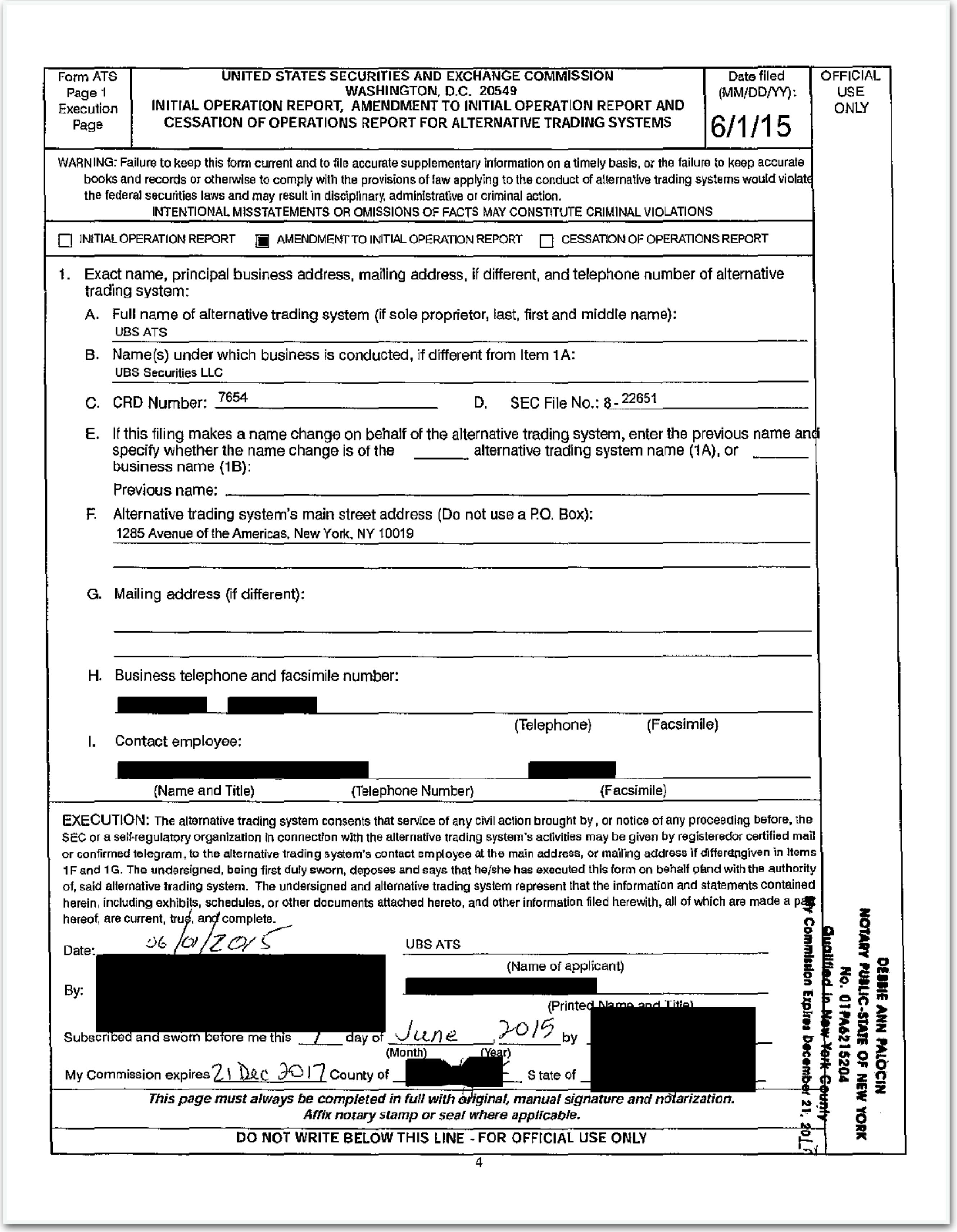
UBS fined $14M by the SEC for issues of unfairness in their dark pool design

We analyzed it, found more issues

First place winner!

620 companies
52 countries

Case Study: UBS ATS



Form ATS Page 1 Execution Page	UNITED STATES SECURITIES AND EXCHANGE COMMISSION WASHINGTON, D.C. 20549 INITIAL OPERATION REPORT, AMENDMENT TO INITIAL OPERATION REPORT AND CESSATION OF OPERATIONS REPORT FOR ALTERNATIVE TRADING SYSTEMS	Date filed (MM/DD/YY): 6/1/15	OFFICIAL USE ONLY

WARNING: Failure to keep this form current and to file accurate supplementary information on a timely basis, or the failure to keep accurate books and records or otherwise to comply with the provisions of law applying to the conduct of alternative trading systems would violate the federal securities laws and may result in disciplinary, administrative or criminal action.

INTENTIONAL MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE CRIMINAL VIOLATIONS

□ INITIAL OPERATION REPORT ☒ AMENDMENT TO INITIAL OPERATION REPORT □ CESSATION OF OPERATIONS REPORT

1. Exact name, principal business address, mailing address, if different, and telephone number of alternative trading system:

A. Full name of alternative trading system (if sole proprietor, last, first and middle name):
UBS ATS

B. Name(s) under which business is conducted, if different from Item 1A:
UBS Securities LLC

C. CRD Number: 7654 D. SEC File No.: 8-22651

E. If this filing makes a name change on behalf of the alternative trading system, enter the previous name and specify whether the name change is of the ______ alternative trading system name (1A), or ______ business name (1B):

Previous name: ______

F. Alternative trading system's main street address (Do not use a P.O. Box):
1285 Avenue of the Americas, New York, NY 10019

G. Mailing address (if different):

H. Business telephone and facsimile number:

[redacted] [redacted]
(Telephone) (Facsimile)

I. Contact employee:

[redacted] [redacted]
(Name and Title) (Telephone Number) (Facsimile)

EXECUTION: The alternative trading system consents that service of any civil action brought by, or notice of any proceeding before, the SEC or a self-regulatory organization in connection with the alternative trading system's activities may be given by registeredor certified mail or confirmed telegram, to the alternative trading system's contact employee at the main address, or mailing address if differengiven in Items 1F and 1G. The undersigned, being first duly sworn, deposes and says that he/she has executed this form on behalf ofand with the authority of, said alternative trading system. The undersigned and alternative trading system represent that the information and statements contained herein, including exhibits, schedules, or other documents attached hereto, and other information filed herewith, all of which are made a part hereof, are current, true, and complete.

Date: 06/01/2015 UBS ATS
(Name of applicant)

By: [redacted] [redacted]
(Printed Name and Title)

Subscribed and sworn before me this 1 day of June, 2015 by [redacted]
(Month) (Year)

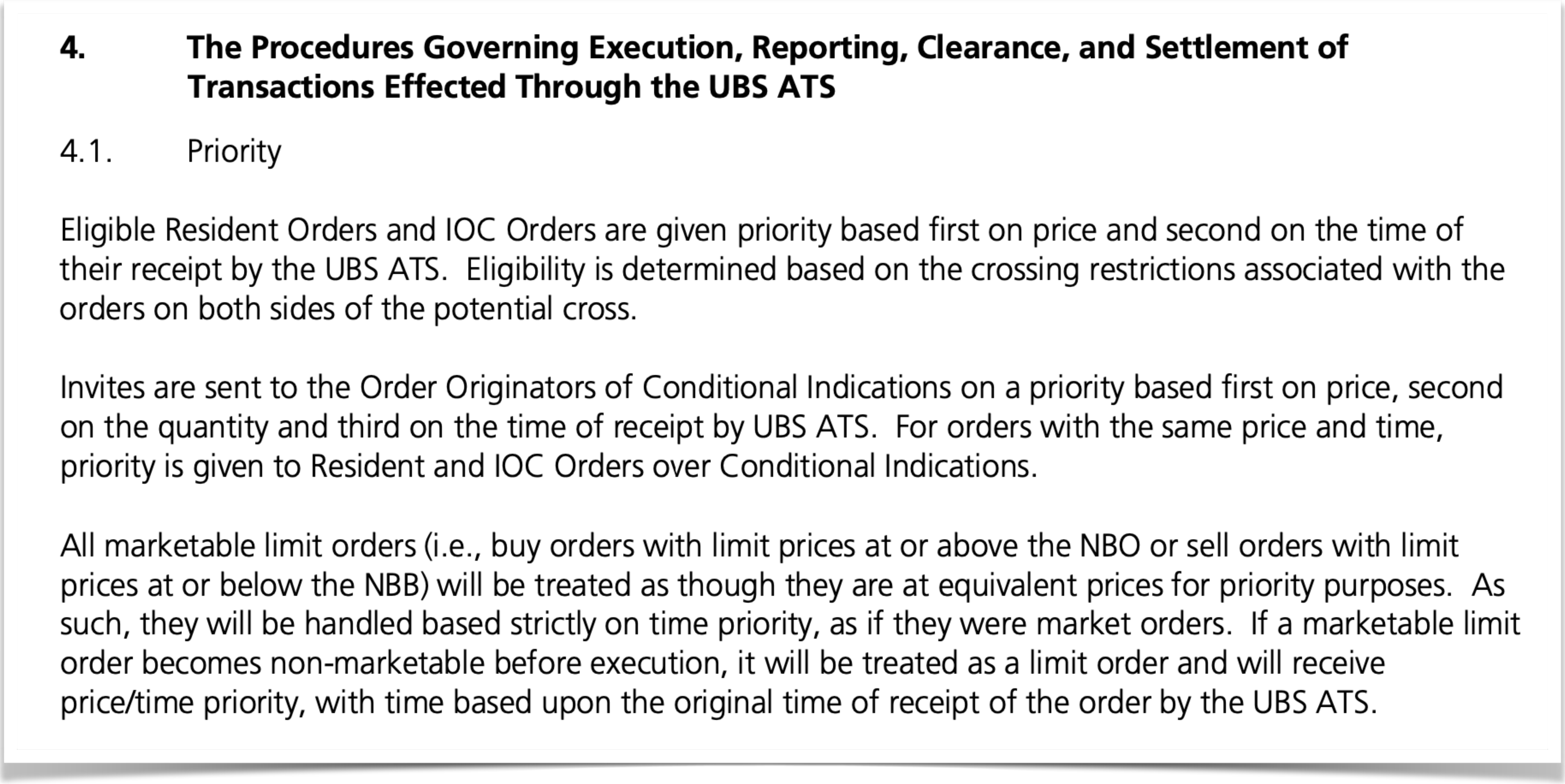
My Commission expires 21 Dec 2017 County of [redacted] State of

This page must always be completed in full with original, manual signature and notarization.
Affix notary stamp or seal where applicable.

DO NOT WRITE BELOW THIS LINE - FOR OFFICIAL USE ONLY

DEBBIE ANN PALOCIN
NOTARY PUBLIC-STATE OF NEW YORK
No. 01PA6215204
Qualified in New York County
My Commission Expires December 21, 2017

4



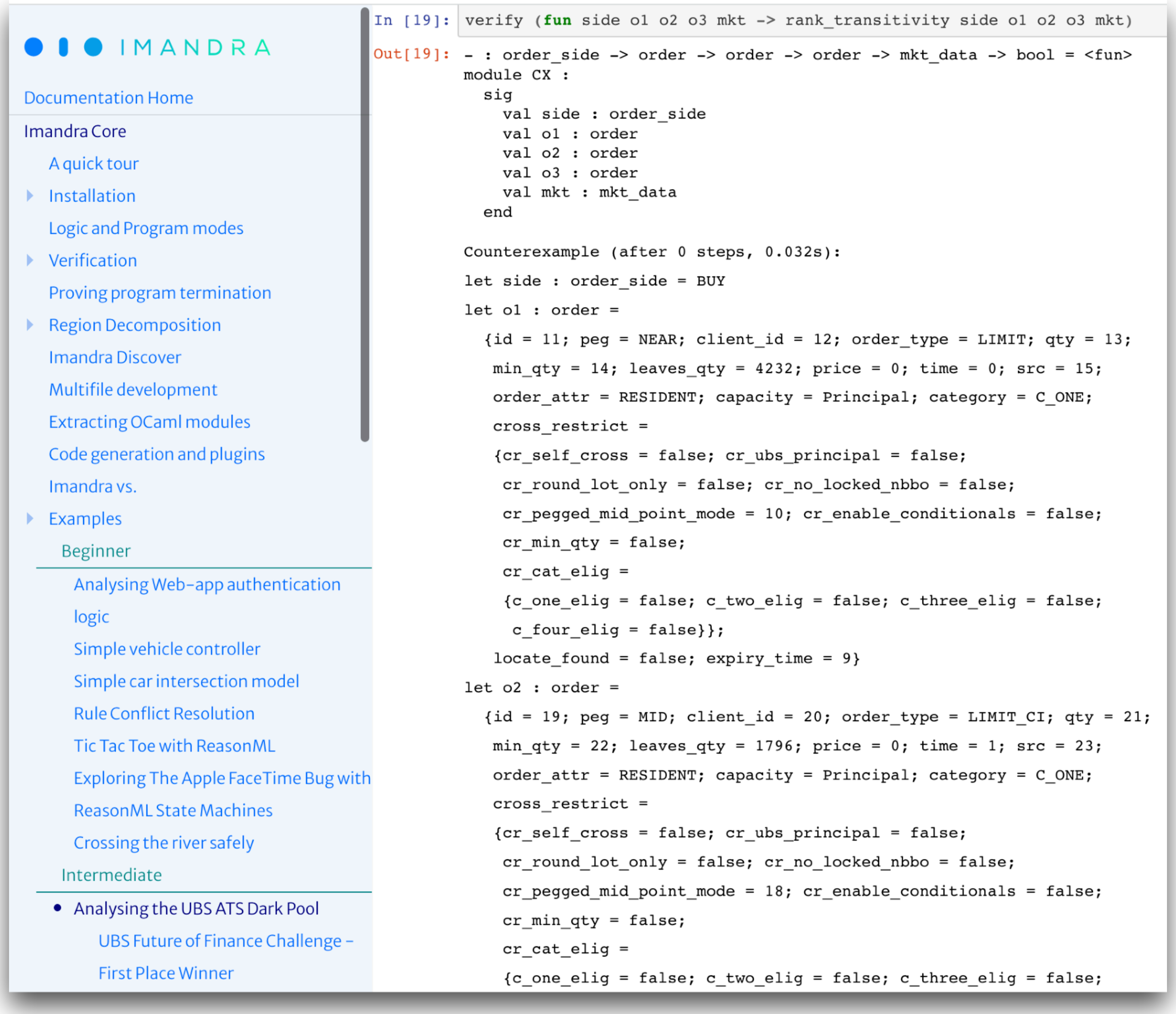
4. The Procedures Governing Execution, Reporting, Clearance, and Settlement of Transactions Effected Through the UBS ATS

4.1. Priority

Eligible Resident Orders and IOC Orders are given priority based first on price and second on the time of their receipt by the UBS ATS. Eligibility is determined based on the crossing restrictions associated with the orders on both sides of the potential cross.

Invites are sent to the Order Originators of Conditional Indications on a priority based first on price, second on the quantity and third on the time of receipt by UBS ATS. For orders with the same price and time, priority is given to Resident and IOC Orders over Conditional Indications.

All marketable limit orders (i.e., buy orders with limit prices at or above the NBO or sell orders with limit prices at or below the NBB) will be treated as though they are at equivalent prices for priority purposes. As such, they will be handled based strictly on time priority, as if they were market orders. If a marketable limit order becomes non-marketable before execution, it will be treated as a limit order and will receive price/time priority, with time based upon the original time of receipt of the order by the UBS ATS.



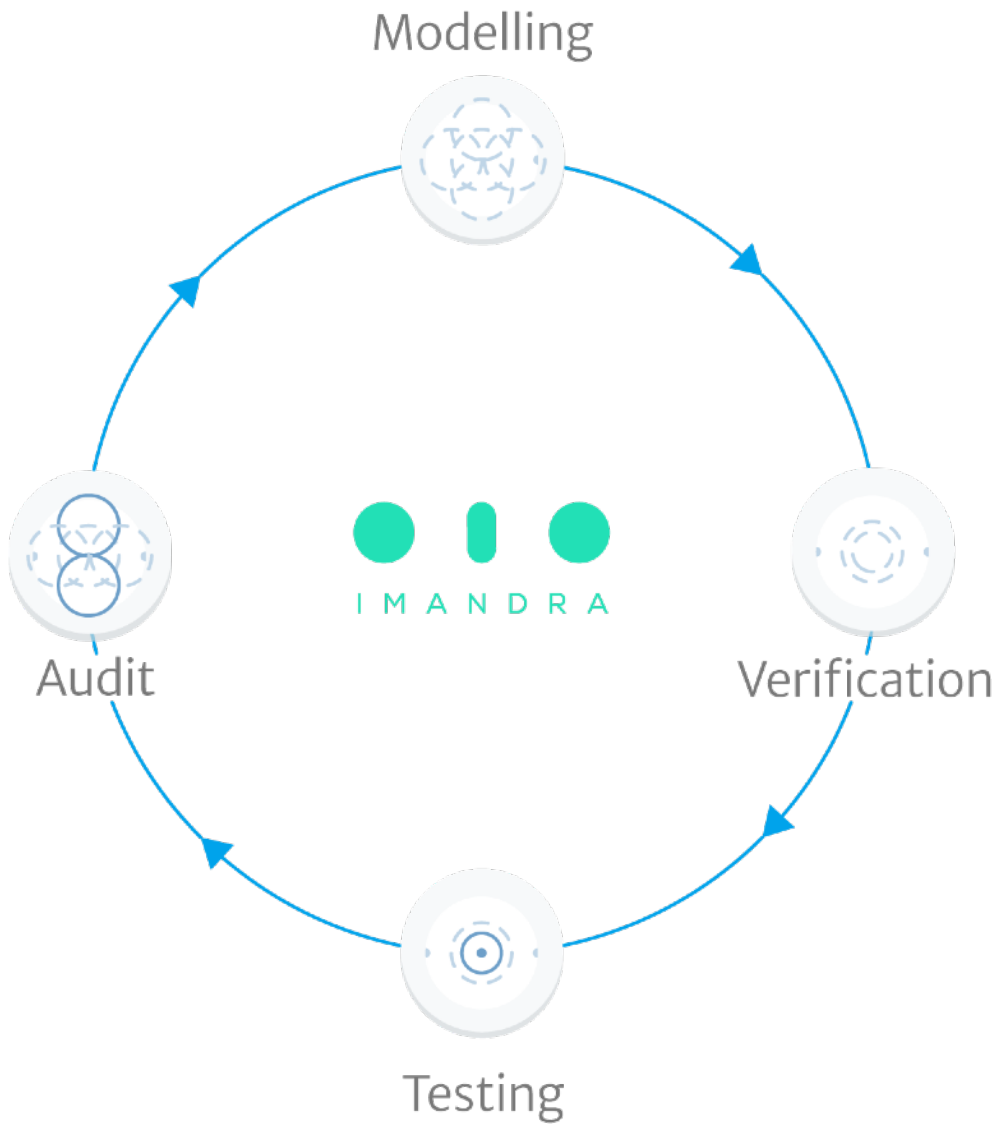
IMANDRA

- Documentation Home
- Imandra Core
  - A quick tour
  - Installation
  - Logic and Program modes
  - Verification
  - Proving program termination
  - Region Decomposition
  - Imandra Discover
  - Multifile development
  - Extracting OCaml modules
  - Code generation and plugins
  - Imandra vs.
  - Examples
    - Beginner
      - Analysing Web-app authentication logic
      - Simple vehicle controller
      - Simple car intersection model
      - Rule Conflict Resolution
      - Tic Tac Toe with ReasonML
      - Exploring The Apple FaceTime Bug with
      - ReasonML State Machines
      - Crossing the river safely
    - Intermediate
      - Analysing the UBS ATS Dark Pool
        - UBS Future of Finance Challenge – First Place Winner

```
In [19]: verify (fun side o1 o2 o3 mkt -> rank_transitivity side o1 o2 o3 mkt)
```

```
Out[19]: - : order_side -> order -> order -> order -> mkt_data -> bool = <fun>
         module CX :
           sig
             val side : order_side
             val o1 : order
             val o2 : order
             val o3 : order
             val mkt : mkt_data
           end

         Counterexample (after 0 steps, 0.032s):
         let side : order_side = BUY
         let o1 : order =
           {id = 11; peg = NEAR; client_id = 12; order_type = LIMIT; qty = 13;
            min_qty = 14; leaves_qty = 4232; price = 0; time = 0; src = 15;
            order_attr = RESIDENT; capacity = Principal; category = C_ONE;
            cross_restrict =
            {cr_self_cross = false; cr_ubs_principal = false;
             cr_round_lot_only = false; cr_no_locked_nbbo = false;
             cr_pegged_mid_point_mode = 10; cr_enable_conditionals = false;
             cr_min_qty = false;
             cr_cat_elig =
             {c_one_elig = false; c_two_elig = false; c_three_elig = false;
              c_four_elig = false}};
            locate_found = false; expiry_time = 9}
         let o2 : order =
           {id = 19; peg = MID; client_id = 20; order_type = LIMIT_CI; qty = 21;
            min_qty = 22; leaves_qty = 1796; price = 0; time = 1; src = 23;
            order_attr = RESIDENT; capacity = Principal; category = C_ONE;
            cross_restrict =
            {cr_self_cross = false; cr_ubs_principal = false;
             cr_round_lot_only = false; cr_no_locked_nbbo = false;
             cr_pegged_mid_point_mode = 18; cr_enable_conditionals = false;
             cr_min_qty = false;
             cr_cat_elig =
             {c_one_elig = false; c_two_elig = false; c_three_elig = false;
```

End-to-End Algorithm Governance



- *Modelling - An **executable formal model** of the trading algorithm. This is tied directly to the specifications given in regulatory filings.*

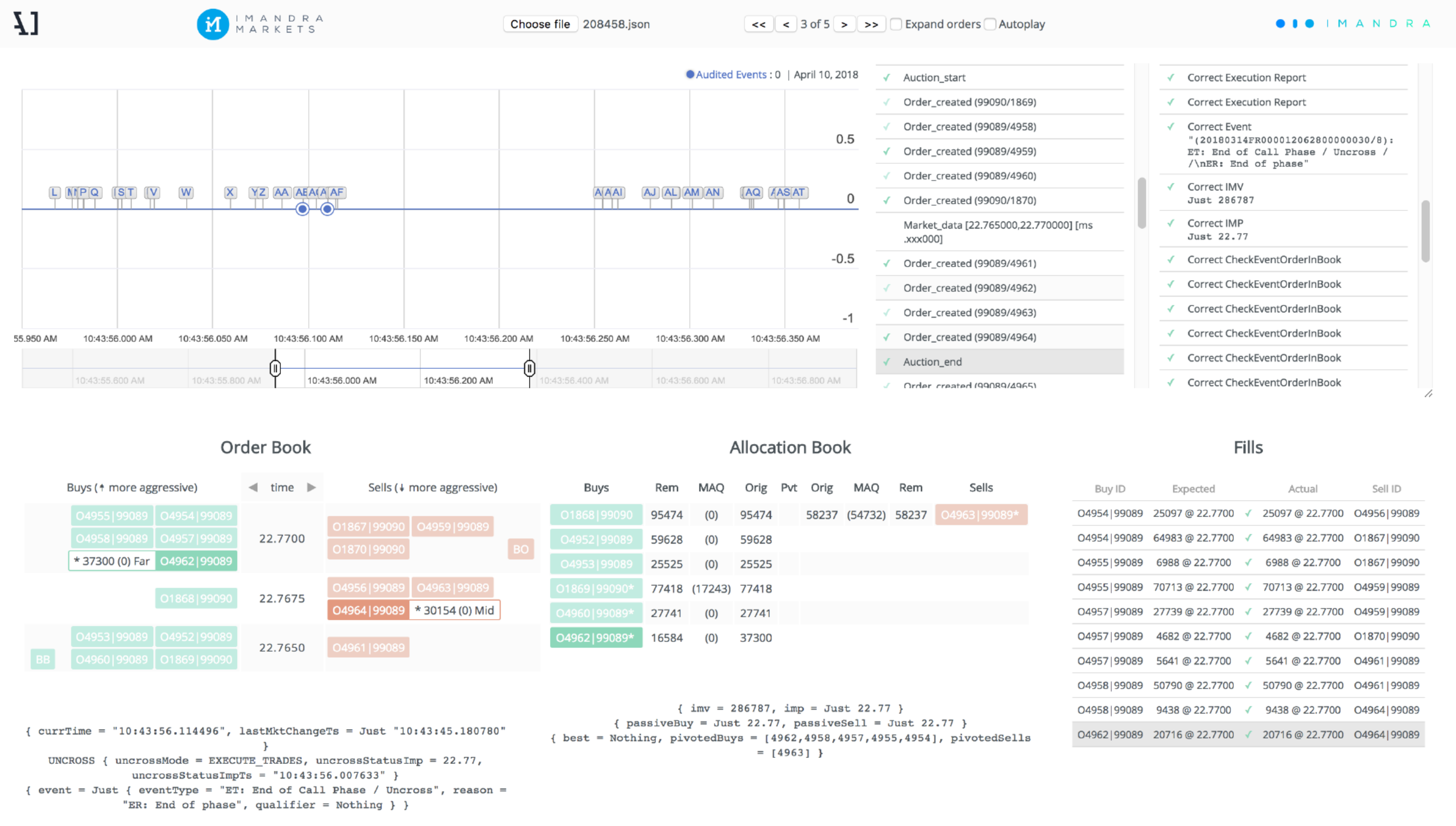
- *Verification - a set of (eventually proven) Verification Goals pertaining to precise behaviour of the model derived from regulations (e.g., MiFID-II and Reg ATS-N). **Counterexamples are crucial** in iterations of system design!*

- *Testing - high coverage testing of the system for conformance with verified design. Test suites **automatically derived** from state-space decompositions of the verified model.*

- *Audit - systematic audit of trading behavior allowing firms and regulators to **quickly detect and investigate behavioural deviations** between the verified design and production system.*

Auditing Algorithms

Interactive visual interfaces are key for investigating discrepancies between verified designs and their production implementations.



- ✓ Auction_start
- ✓ Order_created (99090/1869)
- ✓ Order_created (99089/4958)
- ✓ Order_created (99089/4959)
- ✓ Order_created (99089/4960)
- ✓ Order_created (99090/1870)
- Market_data [22.765000,22.770000] [ms .xxx000]
- ✓ Order_created (99089/4961)
- ✓ Order_created (99089/4962)
- ✓ Order_created (99089/4963)
- ✓ Order_created (99089/4964)
- ✓ Auction_end
- ✓ Order_created (99089/4965)

- ✓ Correct Execution Report
- ✓ Correct Execution Report
- ✓ Correct Event
  ```
  "(20180314FR0000120628000000030/8):
  ET: End of Call Phase / Uncross /
  /\nER: End of phase"
  ```
- ✓ Correct IMV
  `Just 286787`
- ✓ Correct IMP
  `Just 22.77`
- ✓ Correct CheckEventOrderInBook
- ✓ Correct CheckEventOrderInBook
- ✓ Correct CheckEventOrderInBook
- ✓ Correct CheckEventOrderInBook
- ✓ Correct CheckEventOrderInBook
- ✓ Correct CheckEventOrderInBook

Order Book

	Buys (↑ more aggressive)	◀ time ▶	Sells (↓ more aggressive)	
	O4955|99089 O4954|99089 O4958|99089 O4957|99089 * 37300 (0) Far O4962|99089	22.7700	O1867|99090 O4959|99089 O1870|99090	BO
	O1868|99090	22.7675	O4956|99089 O4963|99089 O4964|99089 * 30154 (0) Mid	
BB	O4953|99089 O4952|99089 O4960|99089 O1869|99090	22.7650	O4961|99089	

```
{ currTime = "10:43:56.114496", lastMktChangeTs = Just "10:43:45.180780"
                                   }
   UNCROSS { uncrossMode = EXECUTE_TRADES, uncrossStatusImp = 22.77,
             uncrossStatusImpTs = "10:43:56.007633" }
{ event = Just { eventType = "ET: End of Call Phase / Uncross", reason =
            "ER: End of phase", qualifier = Nothing } }
```

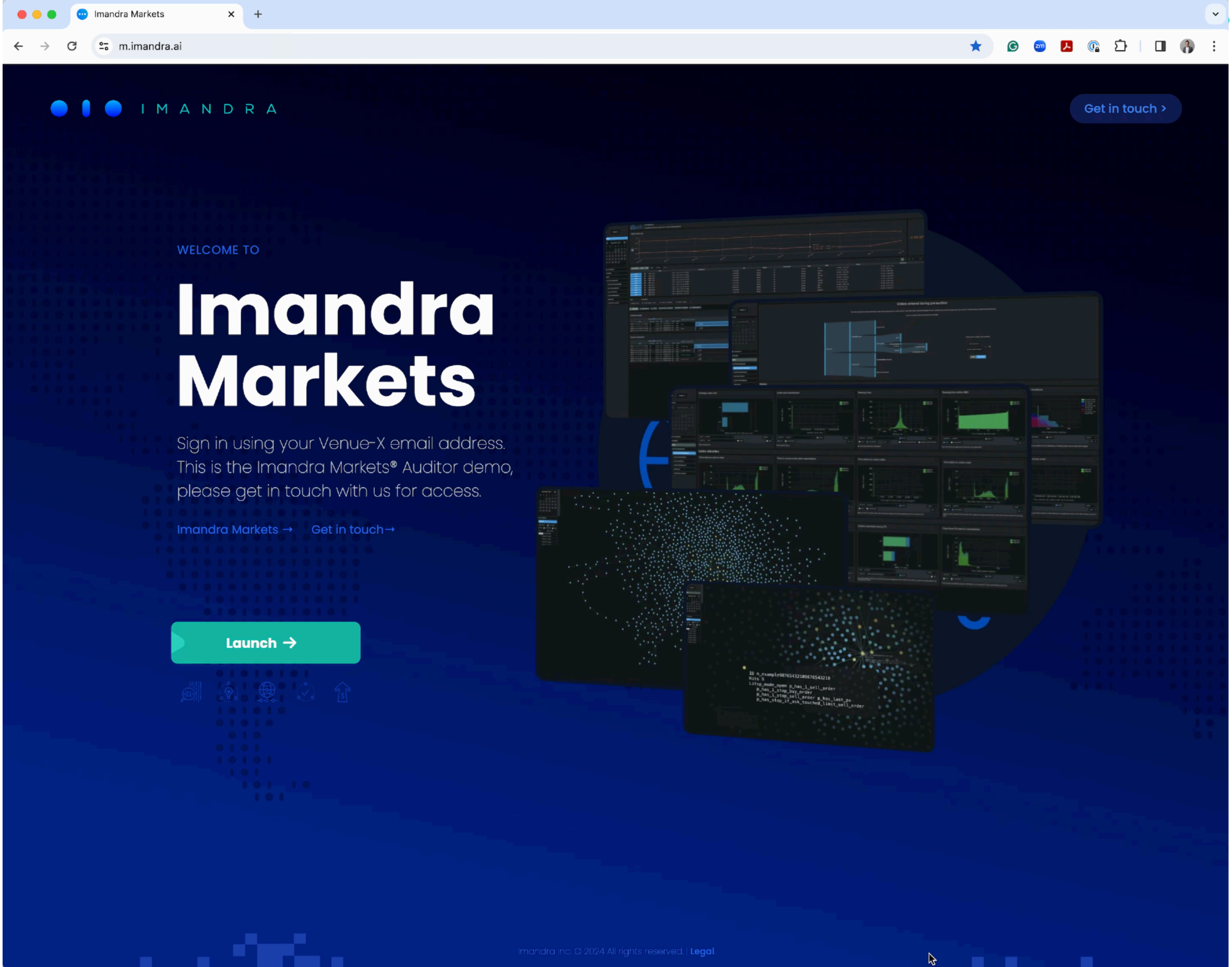
Allocation Book

Buys	Rem	MAQ	Orig	Pvt	Orig	MAQ	Rem	Sells
O1868|99090	95474	(0)	95474		58237	(54732)	58237	O4963|99089*
O4952|99089	59628	(0)	59628					
O4953|99089	25525	(0)	25525					
O1869|99090*	77418	(17243)	77418					
O4960|99089*	27741	(0)	27741					
O4962|99089*	16584	(0)	37300					

```
              { imv = 286787, imp = Just 22.77 }
      { passiveBuy = Just 22.77, passiveSell = Just 22.77 }
{ best = Nothing, pivotedBuys = [4962,4958,4957,4955,4954], pivotedSells
                          = [4963] }
```

Fills

Buy ID	Expected		Actual	Sell ID
O4954|99089	25097 @ 22.7700	✓	25097 @ 22.7700	O4956|99089
O4954|99089	64983 @ 22.7700	✓	64983 @ 22.7700	O1867|99090
O4955|99089	6988 @ 22.7700	✓	6988 @ 22.7700	O1867|99090
O4955|99089	70713 @ 22.7700	✓	70713 @ 22.7700	O4959|99089
O4957|99089	27739 @ 22.7700	✓	27739 @ 22.7700	O4959|99089
O4957|99089	4682 @ 22.7700	✓	4682 @ 22.7700	O1870|99090
O4957|99089	5641 @ 22.7700	✓	5641 @ 22.7700	O4961|99089
O4958|99089	50790 @ 22.7700	✓	50790 @ 22.7700	O4961|99089
O4958|99089	9438 @ 22.7700	✓	9438 @ 22.7700	O4964|99089
O4962|99089	20716 @ 22.7700	✓	20716 @ 22.7700	O4964|99089



WELCOME TO

Imandra Markets

Sign in using your Venue-X email address. This is the Imandra Markets® Auditor demo, please get in touch with us for access.

Imandra Markets → Get in touch→

Conclusion

- Pressing need for:
  - financial infrastructure to be bullet-proof w.r.t. safety and fairness regulations
  - venue matching logics and connectivity protocols to be formally described to regulators and market participants
  - these artifacts to be formally analyzed w.r.t. precise encodings of regulatory directives
- Automated reasoning and formally verified digital twins are transforming this field — *the very foundation of our national financial markets* — by digitizing designs and requirements, and formally verifying trading system behaviors at scale.