



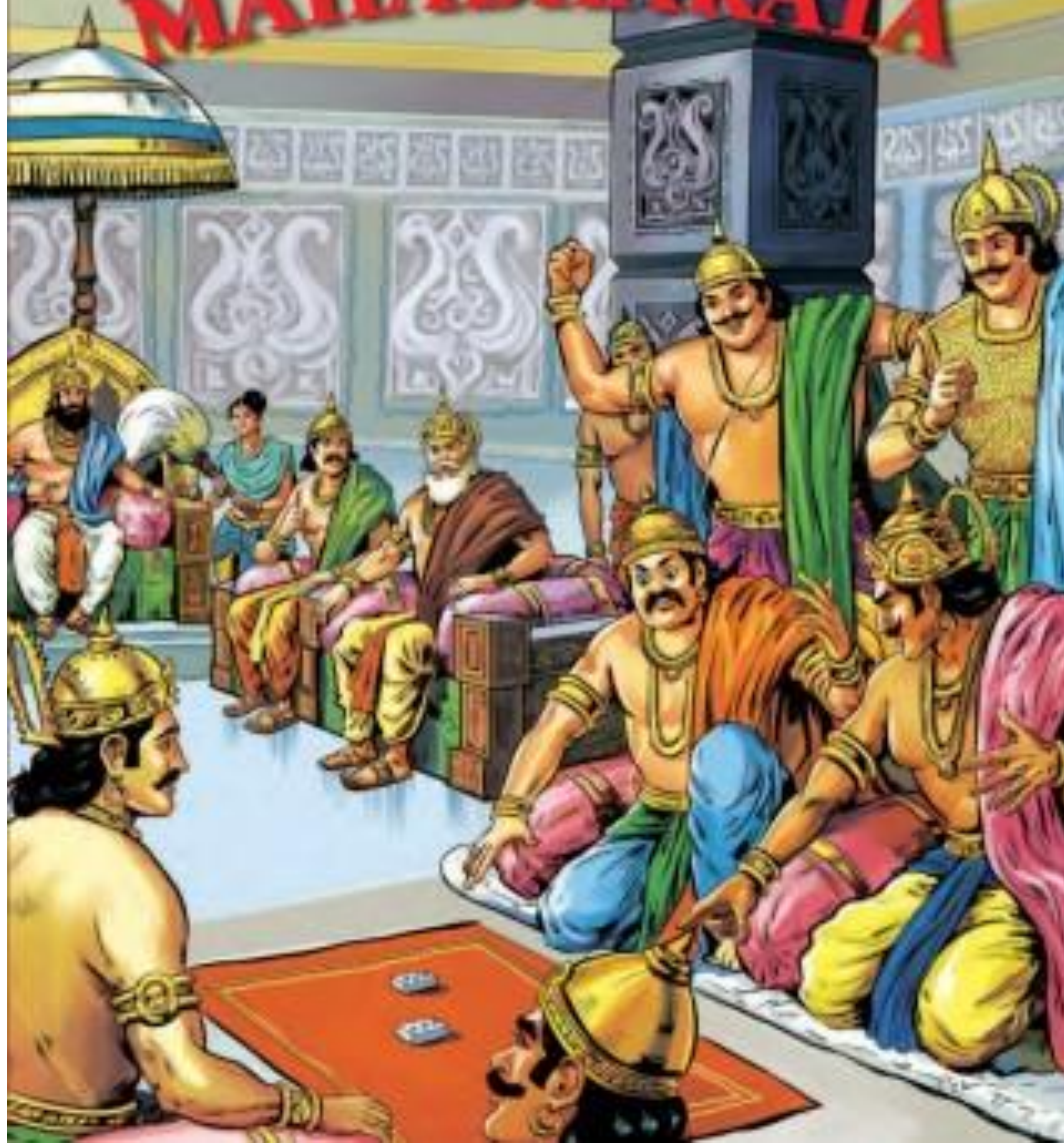
 atul.tripathi2007@gmail.com

 [@quant_guru](https://twitter.com/quant_guru)

 <https://www.linkedin.com/in/atul-tripathi-51438a12/>

AMAR
CHITRA
KATHA

MAHABHARATA



What is Behavioral Analytics?

Definition: Behavioral analytics quantify the effects of psychological, social, cognitive, and emotional factors on human decision-making



We are creatures of habit.



Events, Relationships and Anomalies
(Friends, Supply Chain, Cyber)

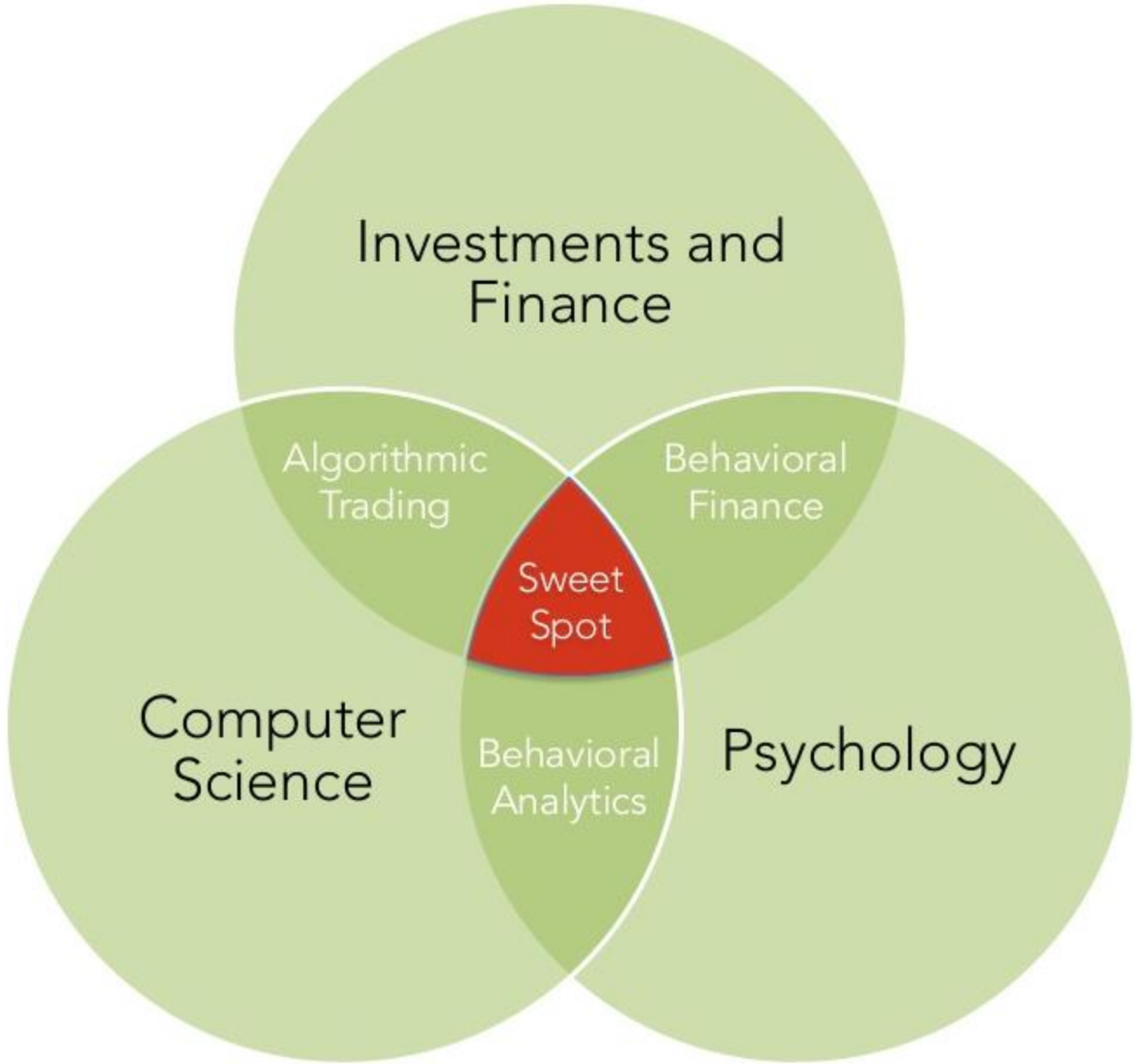
Process Mining: Habits and Behavior
(Shopping Habits, Buying Cycle)



Preferences: Likes and Dislikes
(Advertising, Regulatory Reporting)



Financial Intelligence



Behaviour Analytics + Financial Intelligence

CRM Knowledge
Extraction, Servicing
& Cross-Sell

Customer
Insight

Human
Resources

Recruiting/Retention,
Talent Analytics,
Automated
Management

Fraud/Misconduct
Detection, Credit
Scoring, Wall-Cross

Risk &
Compliance

Market
Intelligence

Behavioral Investing,
Alpha Generation,
Liars Poker



Behavioural Analysis - Enablers




Consolidation of Data Sources

-  Internal Client Data e.g. Know Your Customer (KYC), Fraud and Transaction History.
-  Internal Records, e.g. Internal Watchlists and suspicious Activity Reports (SARs) Records.
-  Data from Governmental Bodies e.g. Watchlists.
-  News and Social Media Searches.
-  Paid for 3rd Party Consumer Data e.g. credit data.
-  Public Domain, e.g. public accounts.

Behavioural Attributes


-  Establish connections with high risk individuals / entities and geographies.
-  Reported to actual income ratio.
-  Geographic, product and behavioral risks.
-  Customers employment industry Sector.
-  Volume, frequency and sentiment of media coverage.

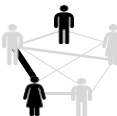
Entity Resolution


-  Ingestion and consolidation of data sets from multiple sources.
-  Link data which references a given customer and deduplicate this data.
-  Create a singular customer view.

Behavioural Analysis – Capabilities


Comparison Against Similar Customers


 A subject runs a convenience store and is grouped into a community based on similarity of the behavioral attributes.


 Analysis identifies that the subject's behavioral attributes are diverging from the expected behavior of the segment with large transactions to an overseas manufacturing firm.

 An alert is generated on this subject for further investigation.


Typology Matching


 Internal data provides a record of transaction history and past case outcomes.


 Subject's behavioral attributes are analyzed for behavioral similarity to subjects upon which cases were previously reported.

 Insights from analysis help with case discounting and alert generation.

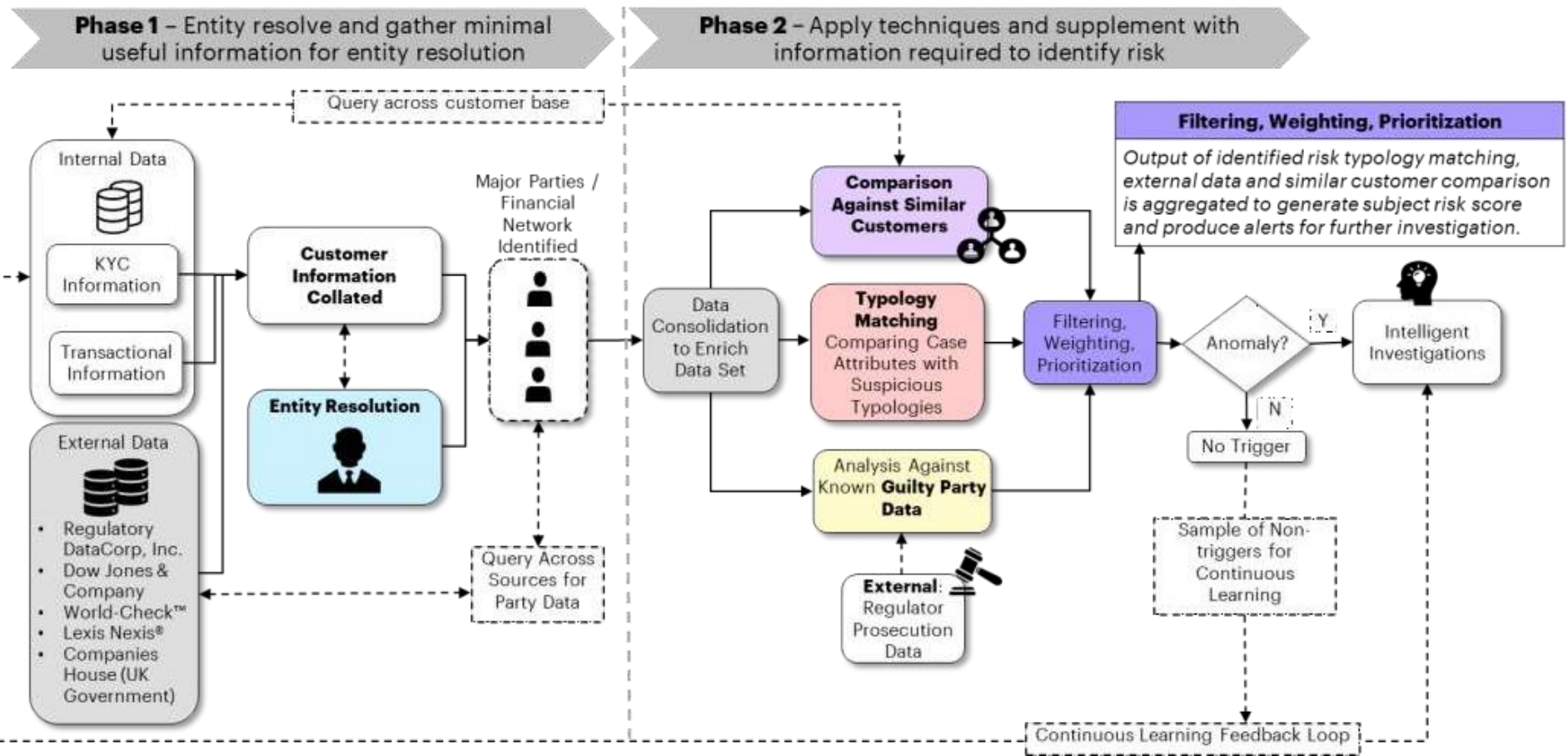
Analysis Against Guilty Party Data

 Ingestion of known guilty party data and associated behavioral attributes.

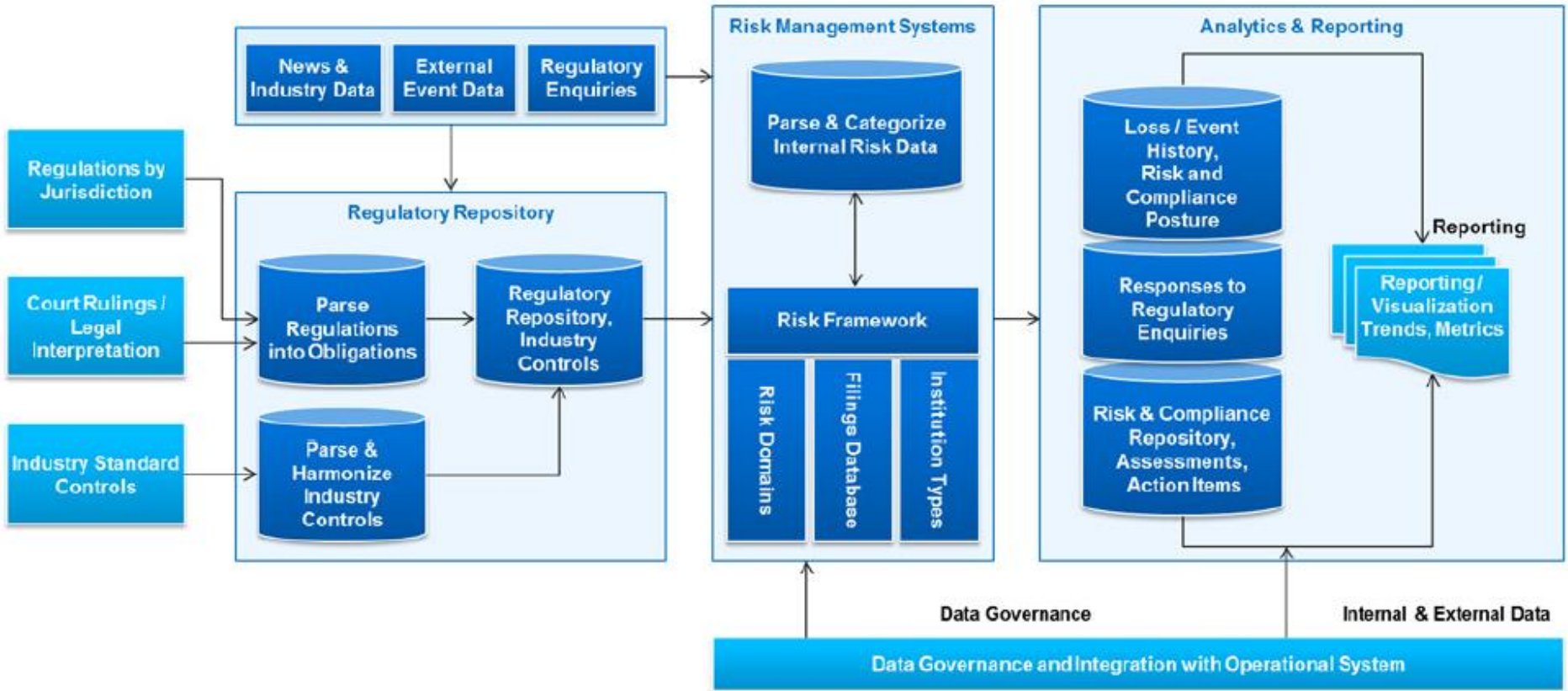
 Subjects in client database are analyzed for behavioral similarity to behavior attributes which indicate a known higher propensity for suspicion.

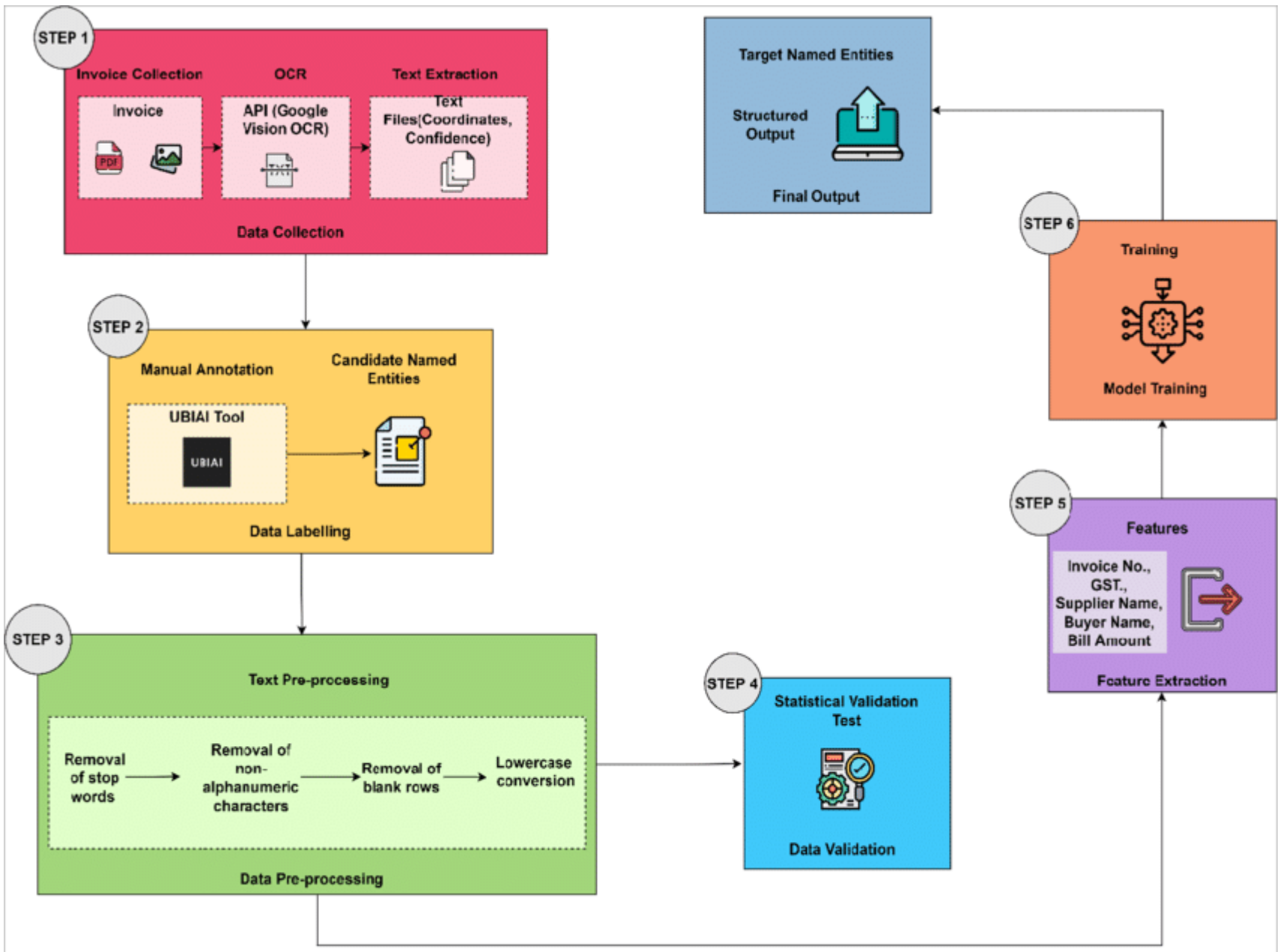
 Insights inform alert generation and prioritization.

Behavioural Analysis - Process Flow



Cognitive Computing – Regulatory Compliance





Cryptocurrency stolen from Delhi lands in Hamas wallets

THE MONEY ROUTE

- ▶ Bizman lost cryptocurrency worth ₹4 crore to hackers in 2019
- ▶ Case filed in west Delhi. Investigation transferred to anti-terror unit-special cell

▶ Probe taken up by IFSO unit in late 2021

▶ The cryptocurrencies landed in suspects' wallets, being used by Hamas

▶ Hamas further transferred some of the funds to a gambling site and a child pornography site



WHAT WAS STOLEN

BITCOIN
at least 6.2

Etherium
9.7

Bitcoin cash
2.4

WHAT INVESTIGATION REVEALED

▶ The Bitcoins were transferred to a private wallet (1P3) and sent further to 1LA belonging to Al-Qassam Brigades

0.2115 bitcoins were transferred to 1Dr (Binance & Coinswitch wallet) of Naseer

Ibrahim Abdulla and was seized by Israel's National Bureau for Counter Terror Financing

2.95 Bitcoins sent to Ahmed Marzooq in Giza, Egypt

9.7 Etherium sent to Ahmed Q H Safi from Ramallah, Palestine

Rajshekhhar Jha
@timesgroup.com

New Delhi: In the winter of 2021, Delhi Police's Special Cell was investigating a case of cryptocurrency theft of around Rs 4 crore from the wallet of a west Delhi businessman. Though the cops managed to 'deep trace' a few recipient wallet IDs, tracking the end users appeared difficult. Just at the time, Israel's intelligence agency, Mossad, communicated — as part of routine intelligence exchange with their Indian counterparts — information about some suspect wallets operated by terrorist groups for terror funding.

Many of the wallet addresses on the list were being operated by the al Qassam brigades of Hamas, the Palestinian terror group, and had been 'seized' by Israel's National Bureau for Counter

Terror Financing

A breakthrough arrived when the Special Cell's Intelligence Fusion & Strategic Ops (IFSO) unit ran a match on the wallets: several wallets that had received the Bitcoin and Ethereum assets from Delhi were operated by the cyber terrorism wing of Hamas.

While Israel has hit back strongly at Hamas for Saturday's attack, sources said the intelligence agencies have their antennae up about renewed efforts by the terror outfit to collect funds by hacking in pro-Israel countries.

Even on Tuesday, the cyber unit of Israel Police froze a large number of cryptocurrency accounts held by Hamas for fundraising. Israel Police said on X that Hamas had launched a crypto fundraising campaign after the start of the latest terror attacks. Israeli authorities also urged crypto exchange Binance to

transfer the seized funds to that country's state treasury.

The case in Delhi was the first instance of Hamas' activity in India. Special Cell officers said that the probe details were communicated to the relevant authorities at the time. Former DCP (Special Cell) KPS Malhotra's team had investigated the case. "Yes, our investigation had led us to several wallets linked to the al Qassam brigades," Malhotra confirmed on Tuesday.

The matter, cops said, was first reported in 2019 at Paschim Vihar police station and the investigation was later transferred to the Special Cell on court orders. After the Hamas link was unearthed, technical analysis revealed that one of the seized wallets belonged to Naseer Ibrahim Abdulla in Gaza and to Hamas operatives like Ahmed Marzooq in Giza and Ahmed QH Safi in Ramallah in Palestine.

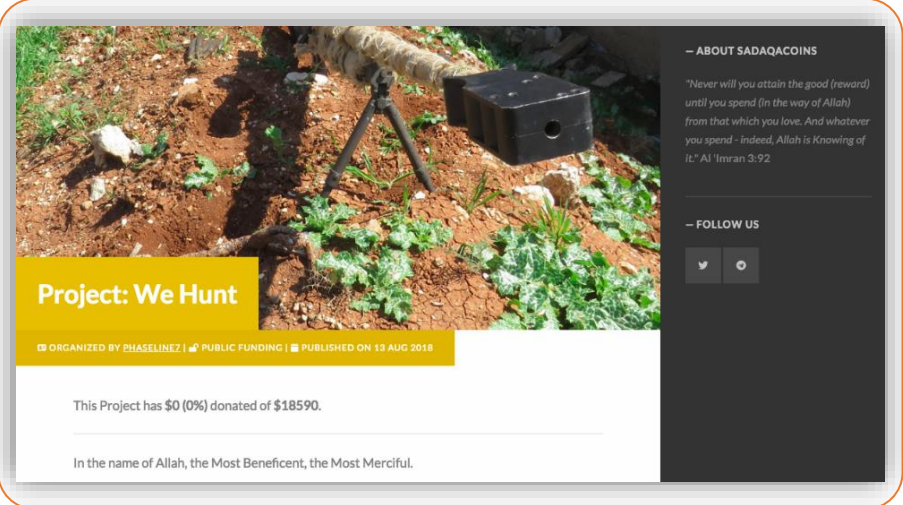
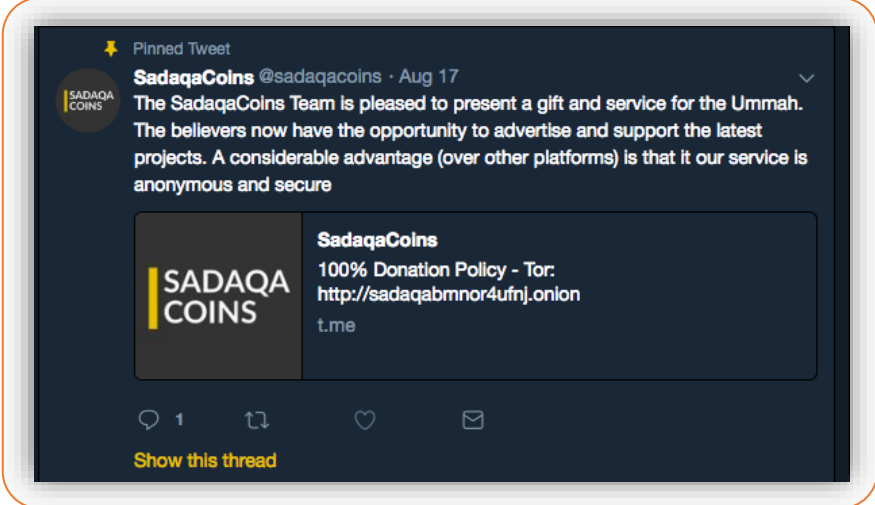
Dark Web – Free market run for everything



ISIS advertising for funds collection; BitCoin key being displayed
Cross platform advertisement – Facebook, WhatsApp, Twitter

ISIS advertising for SadaqaCoins

ISIS using incorrect religious interpretation for justifying collection of funds on DarkWeb





Enterprise Fraud Management

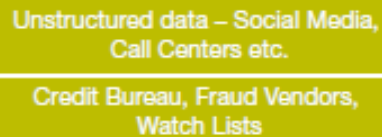


Big Data

Customer View Internal Data



Customer View External Data



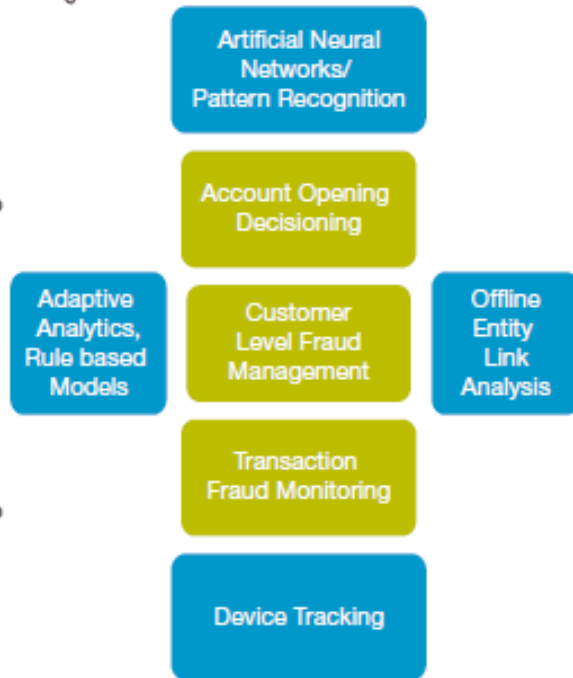
Customer View Transaction Data



Advanced analytics methodologies



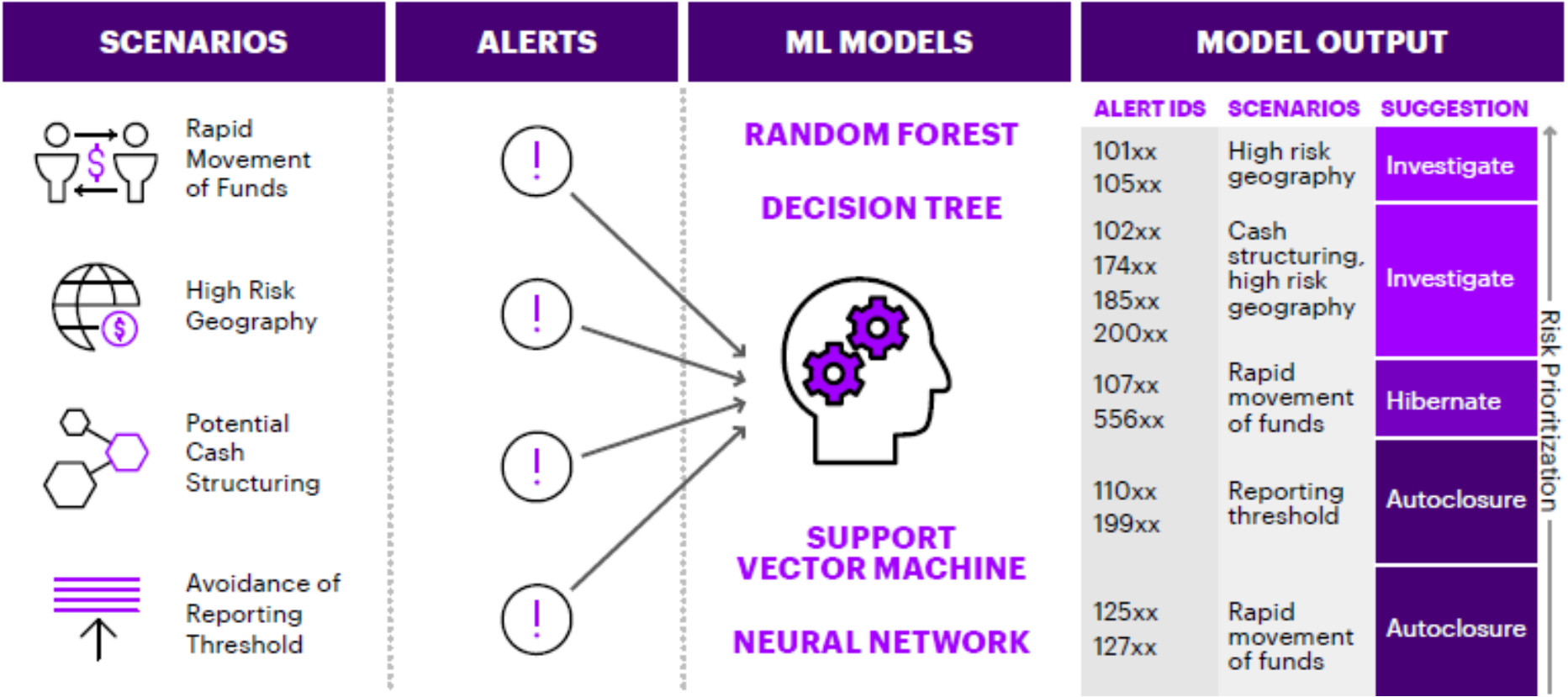
Fraud Monitoring & Detection



Fraud Management Actions



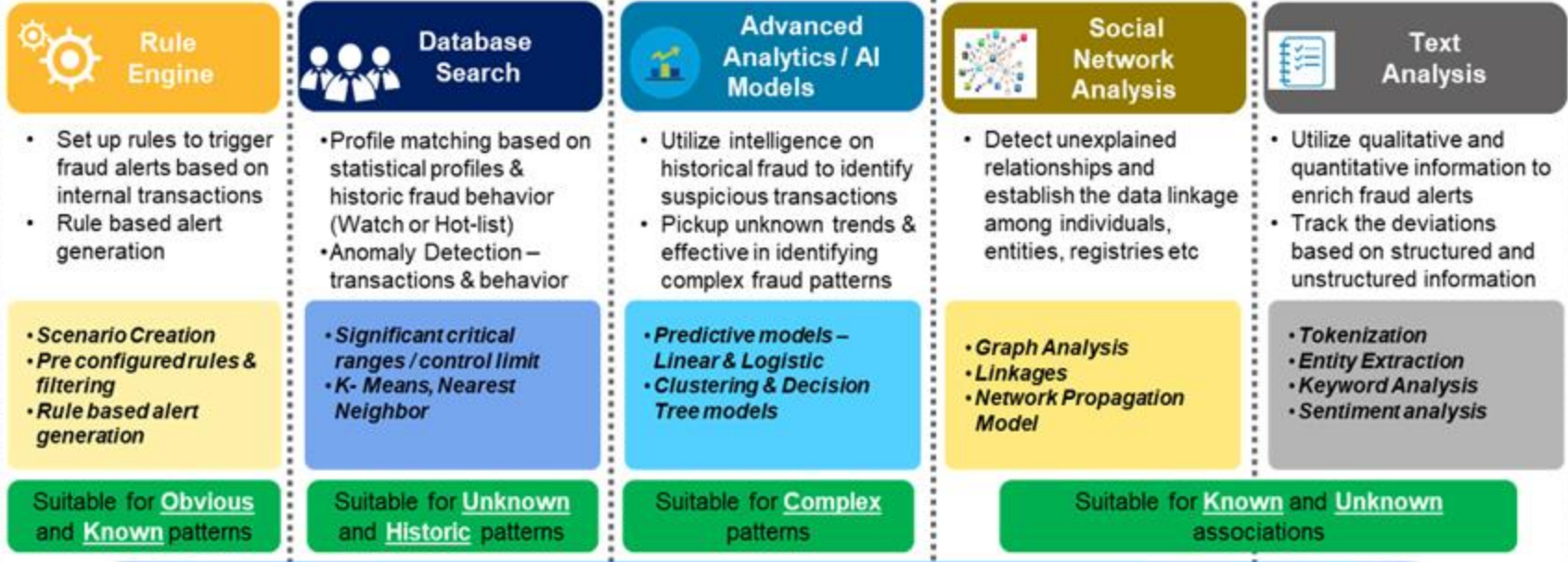
Suspicious Activity Detection – Risk Prioritization Approach



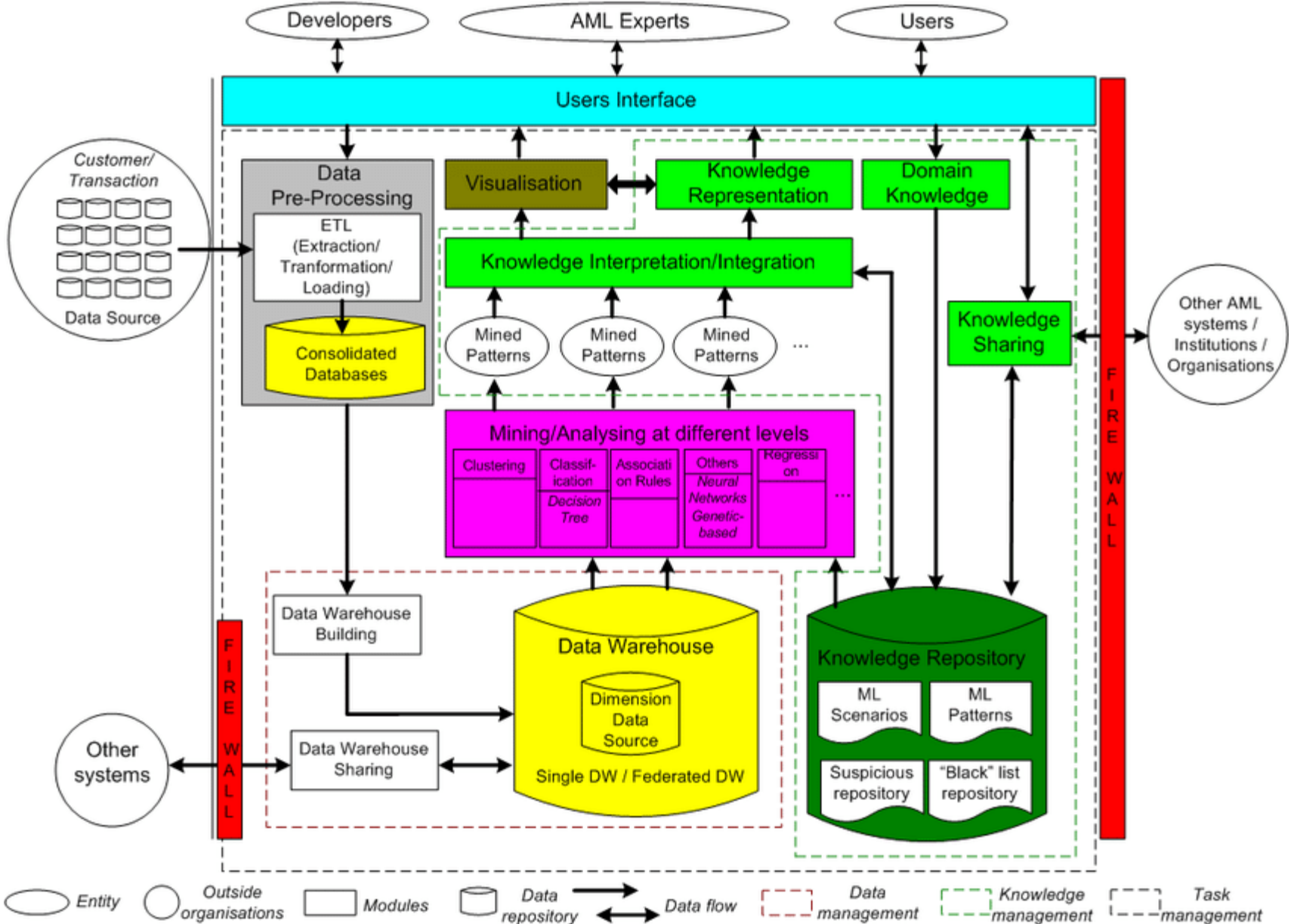
Shell Companies

AI & ML enabled AML Transaction Monitoring

- Identify unknown pattern of fraud
- Early warning of Fraud
- Track new fraud instances
- Streamlined alert management



KDD AML SYSTEM ARCHITECTURE



MT700

-----Instance Type and Transmission-----

Original Received from Application - Outgoing Draft

Priority/Delivery : Normal

-----Message Header-----

Swift Input : FIN 700 Issue of a Documentary Credit

Sender Swift address : AGRIFRPPXXX

BANK ABC, 39th Street, Paris, France

Receiver Swift address : CITIUS32XXX

BANK XYZ CITIUS32, New York, NY 10043

-----User Header-----

Message-User-Reference : 002MSOG1206801JH

-----Message Text-----

:27: Sequence of Total

1/1

:40A: Form of Documentary Credit

IRREVOCABLE

:20: Documentary Credit Number

0021L02120680001

:31C: Date of Issue

120308

:40E: Applicable Rules

UCP LATEST VERSION

:31D: Date and Place of Expiry

120315PARIS

:50: Applicant

BOL INTERNATIONALES SA, 87 RUE DE PARIS

PARC ORSAY, BATIMENT SEQUOIA, BP7, 91402 ORSAY CED X

:59: Beneficiary

STAR INTERNATIONL, 19, 5TH STREET, CHARLESTON ROAD,

MOUNTAIN VIEW

:32B: Currency Code, Amount

USD3000000,

:39A: Percentage Credit Amount Tolerance

10/10

:41A: Available With ... By ...

CITIUS32 BY PAYMENT

:43P: Partial Shipments

ALLOWED

:43T: Transshipment

ALLOWED

:44A: Place of Taking in Charge/Dispatch from .../Place of Receipt

FLORIDA

:44E: Port of Loading/Airport of Departure

SIDNEY, AUSTRALIA

:44F: Port of Discharge/Airport of Destination

GOERGE TOWN

:44B: Place of Final Destination/For Transportation to .../Place of Delivery

PARIS

:44C: Latest Date of Shipment

120310

:45A: Description of Goods and/or Services

FURNITURE AND RAW METRIAL /INCO TERM/ CIF: COST, INSURANCE AND FREIGHT

(NAMED DESTINATION PORT) TRADE TERMS : CIF PARIS

CONTAINS - Office Furniture including Metal Framed Seating, Bedside Chairs, Bariatric

Seating, Oversize Seating and raw materials - hardwood plywood, glass, P205,

fluorophosphate glass, zirconium fluoride

:46A: Documents Required

2COPY(S) PACKING LIST

BENEFICIARY'S PACKING LIST INDICATING THE DETAILS OF THE MATERIALS SHIPPED AS MENTIONED UNDER THE CONTRACT

+2COPY(S) INVOICE

SIGNED COMMERCIAL INVOICE IN TWO COPIES INDICATING THIS CREDIT NUMBER

+1/2 ORIGINAL(S) AND 2 COPY(S) SEAWAY DOCUMENTS

COPY OF FAX/TELEX ADVISING APPLICANT PARTICULARS OF SHIPMENT INCLUDING B/L

NO., DATE, VESSEL NAME, NATIONALITY, PORT OF LOADING AND DISCHARGE,

SHIPMENT DATE WITHIN FIVE WORKING DAYS AFTER SHIPMENT DATE

+1/2 ORIGINAL(S) AND 2 COPY(S) AIRWAY DOCUMENTS

CLEAN AIRWAY BILL CONSIGNED TO THE APPLICANT, NOTIFY

APPLICANT MARKED F73, INDICATING THIS CREDIT NUMBER

:48: Period for Presentation

5

:49: Confirmation Instructions

WITHOUT

:78: Instructions to the Paying/Accepting/Negotiating Bank

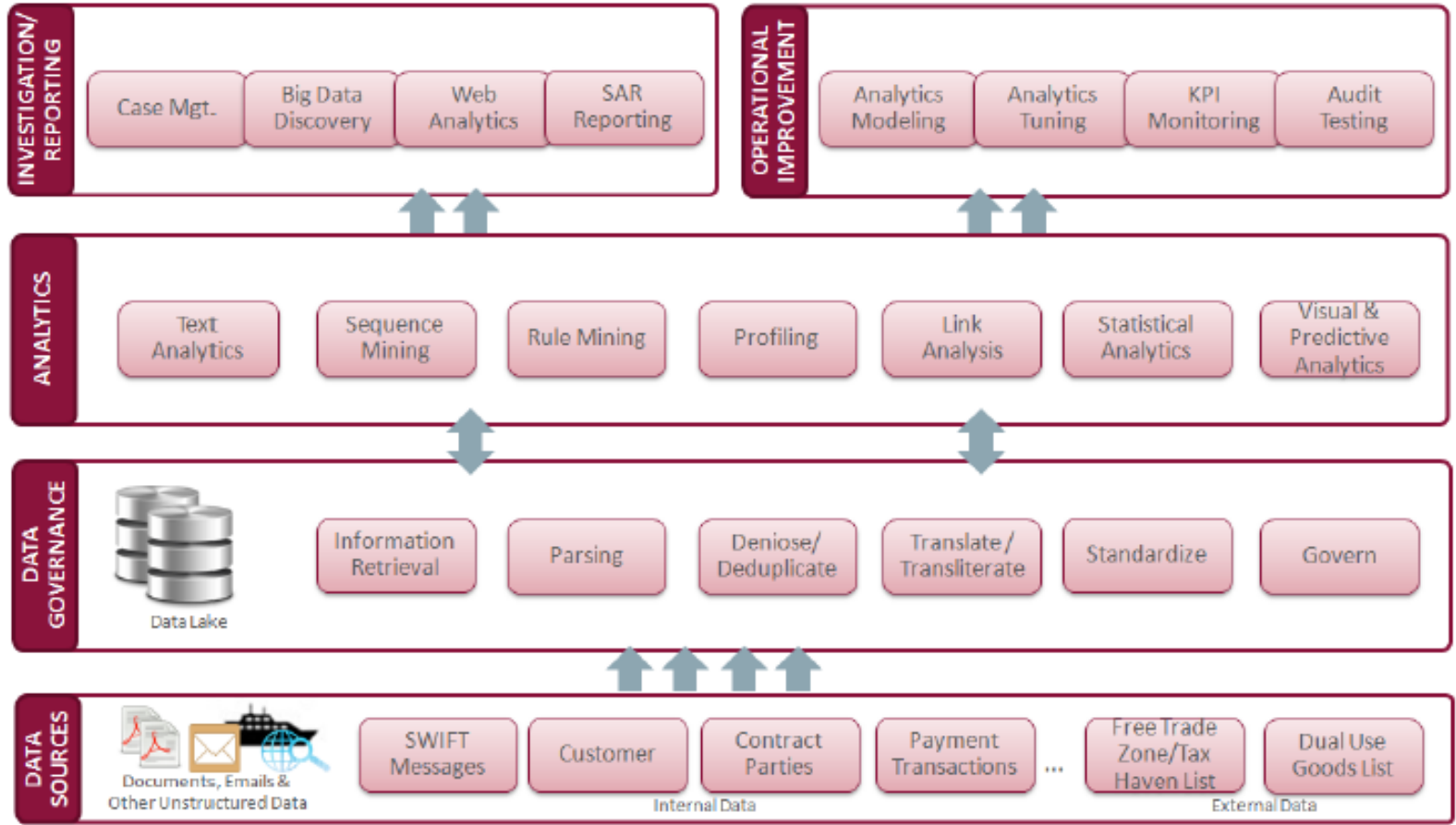
+PLEASE FORWARD ALL DOCUMENTS TO US BY COURIER SERVICES IN ONE LOT.

+ON RECEIPT OF DOCUMENTS COMPLYING PRESENTATION, WE SHALL REMIT THE

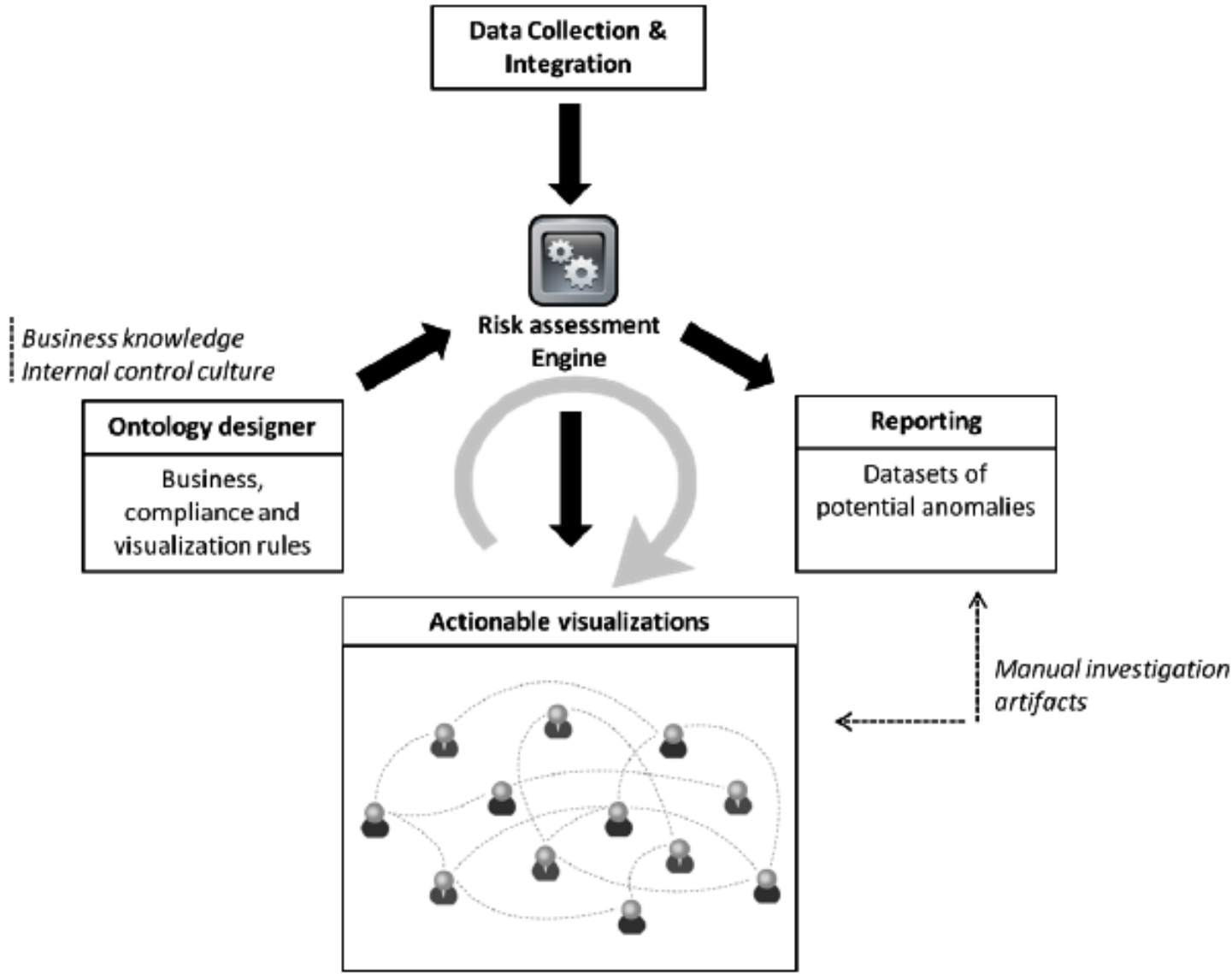
PROCEEDS IN ACCORDANCE WITH THE INSTRUCTIONS OF THE

NEGOTIATING/PRESENTING BANK.

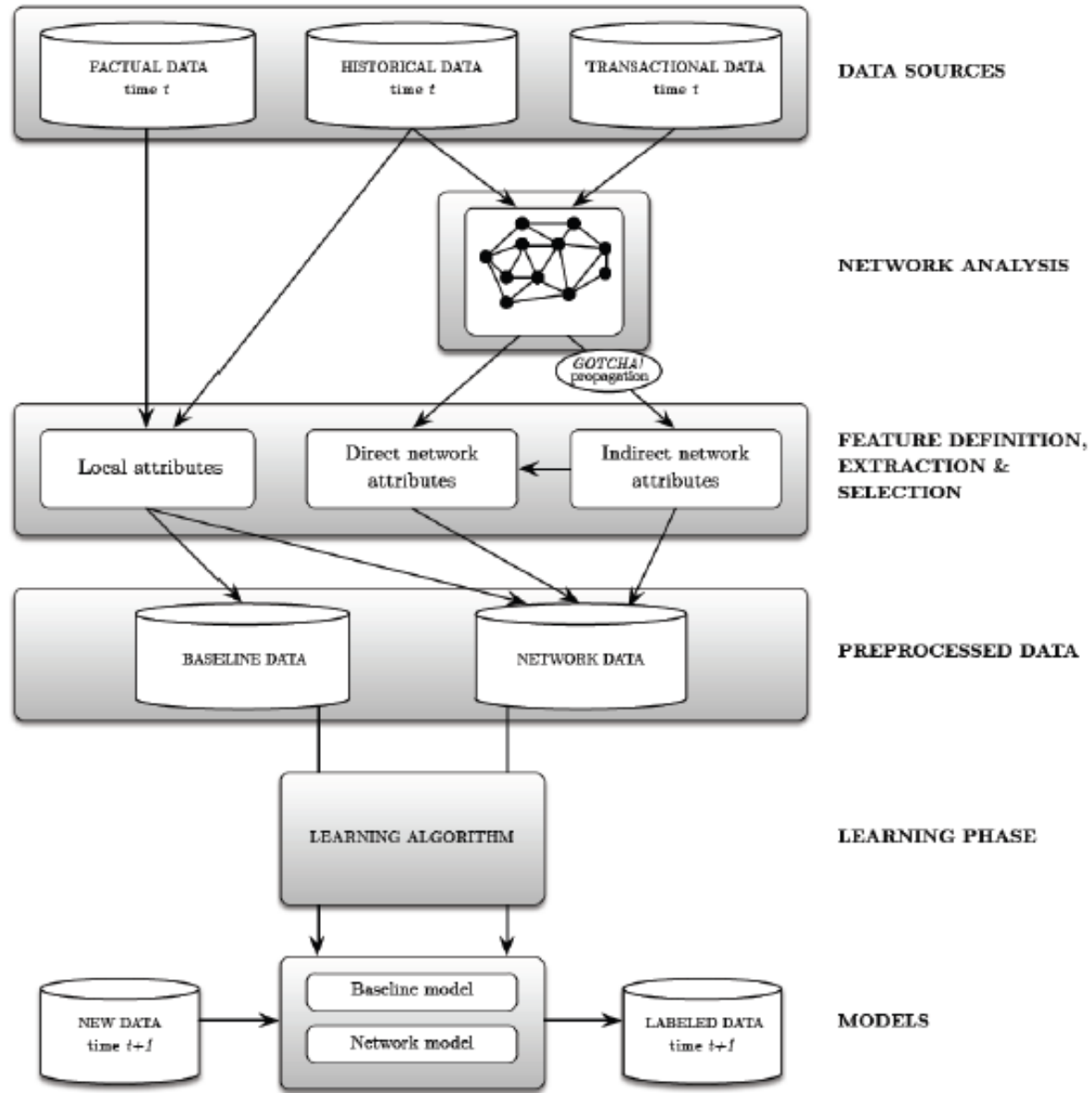
Framework – TBML



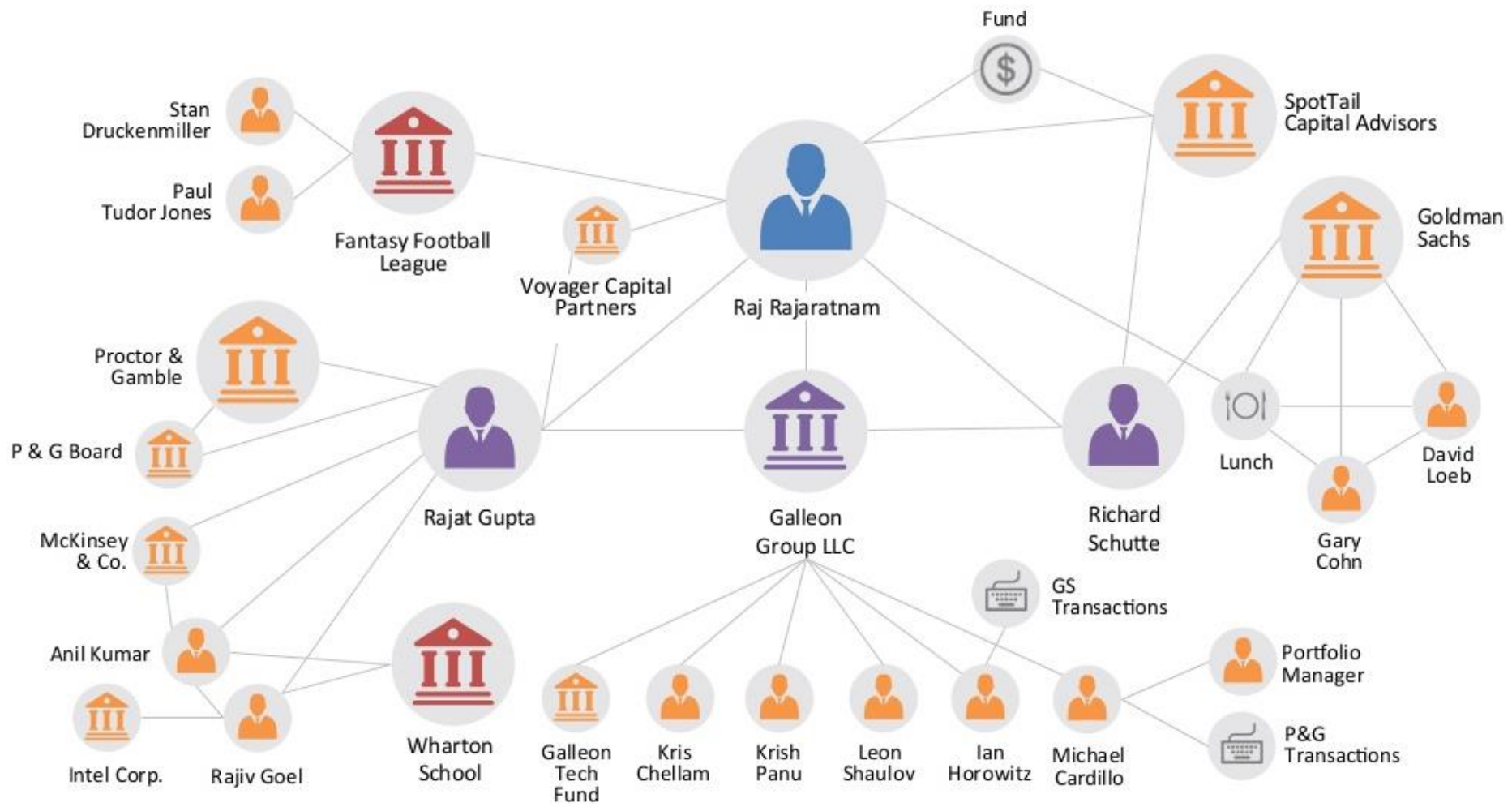
Fraud Detection by Social Network Analysis



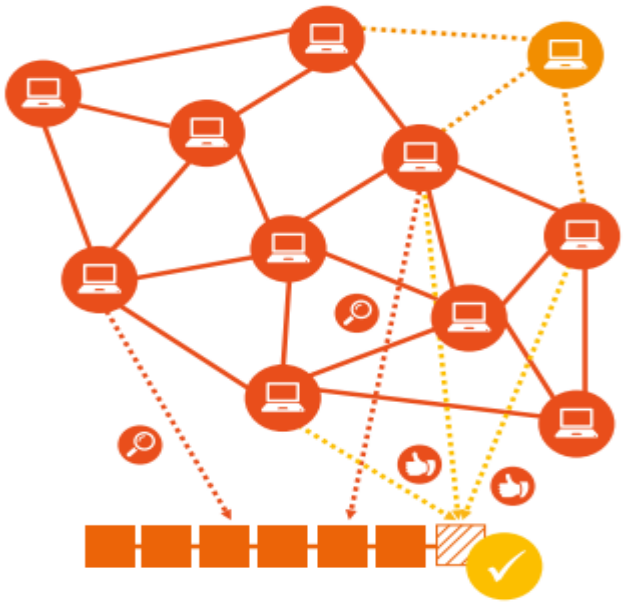
Fraud Detection Techniques using Social Network Analysis



Knowledge Graph



Categories of Block chain



PUBLIC BLOCKCHAIN

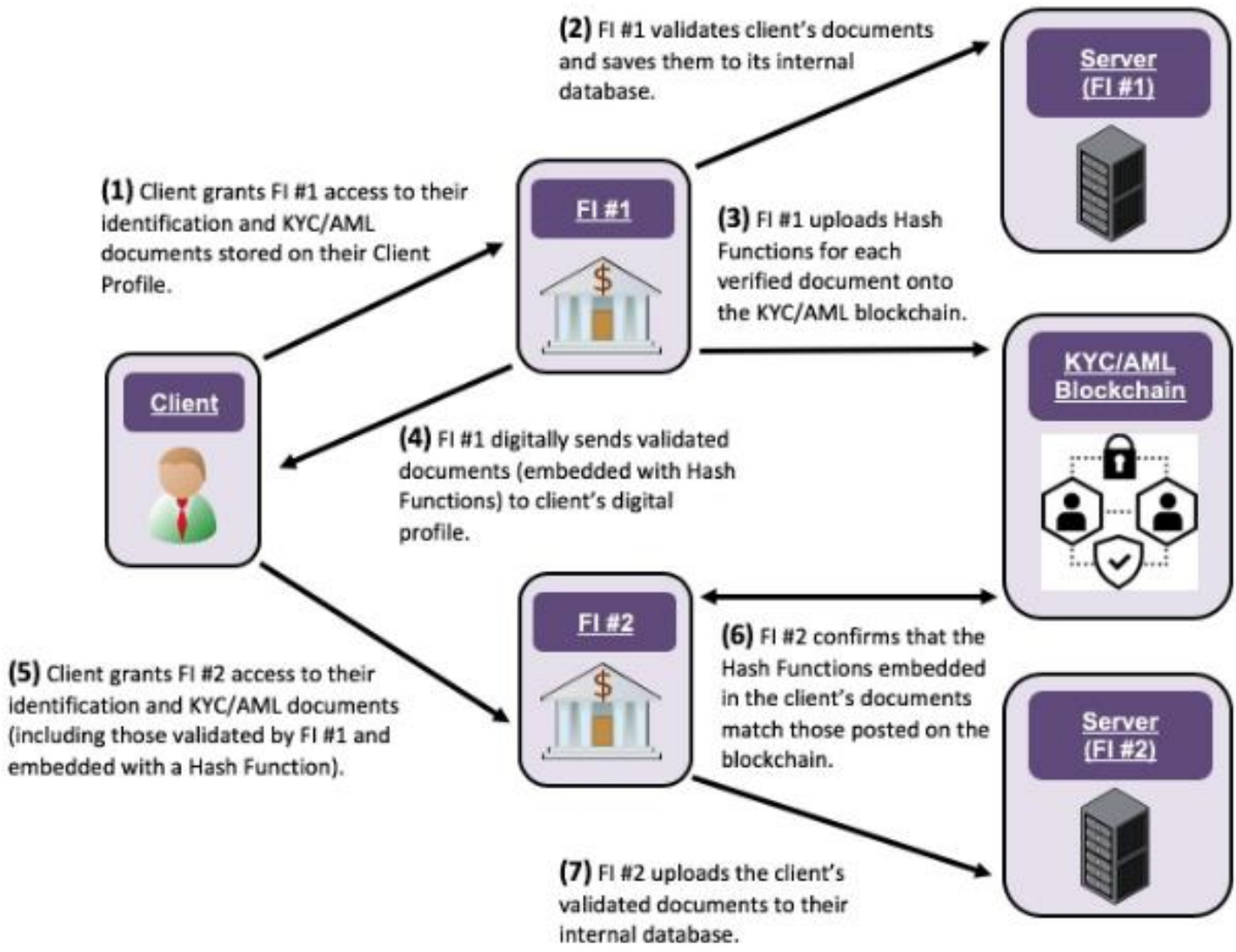


PRIVATE BLOCKCHAIN

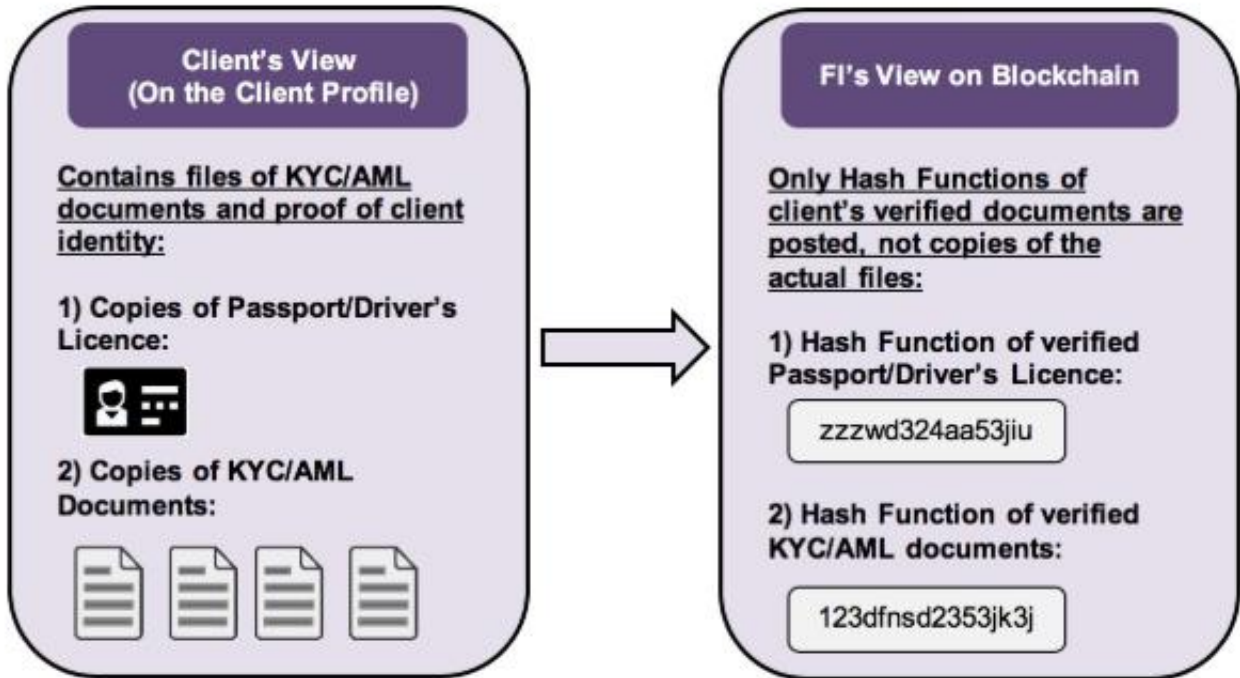


CONSORTIUM BLOCKCHAIN

Block chain for KYC/AML compliance



Block chain legal and business challenges



Standardizing KYC/AML Documentation

Ensuring the Validity of Verified KYC/AML Data Stored on the DLT Platform

Data Privacy Concerns for Data Stored on the Blockchain

Incentivizing the Sharing of Information Between FIs

Block chain for Anti Money Laundering

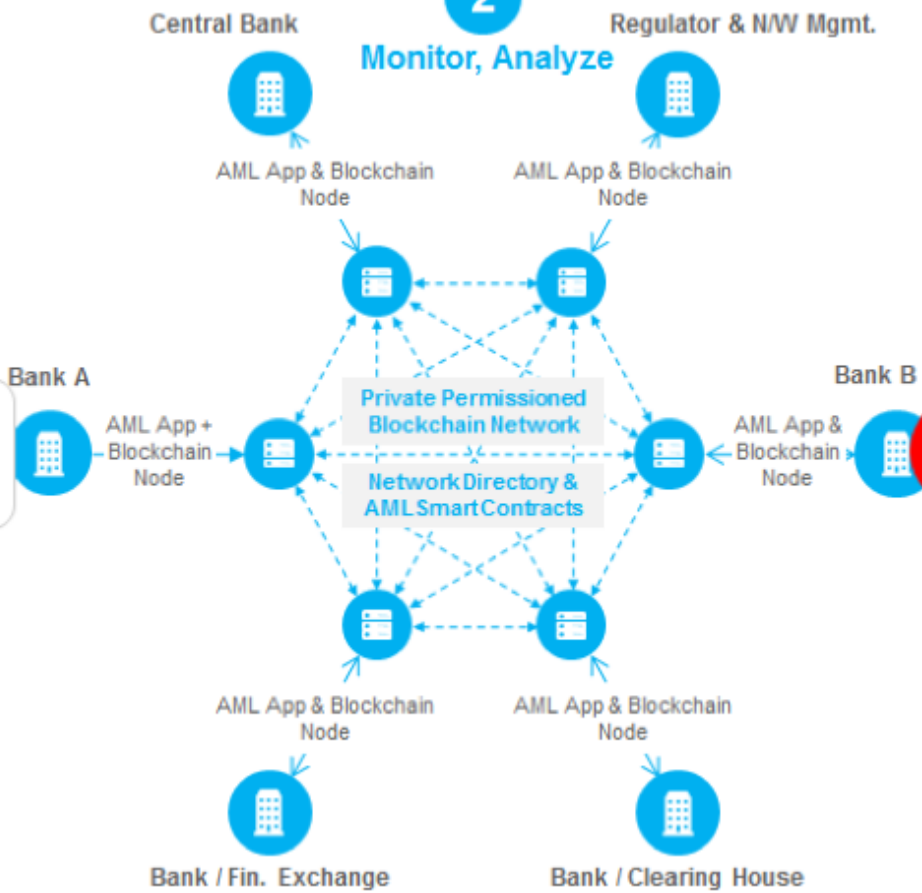
1 Input subset of transactions



Input data.
Invoke smart contract

- Transaction/payments
- Customer profile data
- Patterns
- Other details

2 Monitor, Analyze



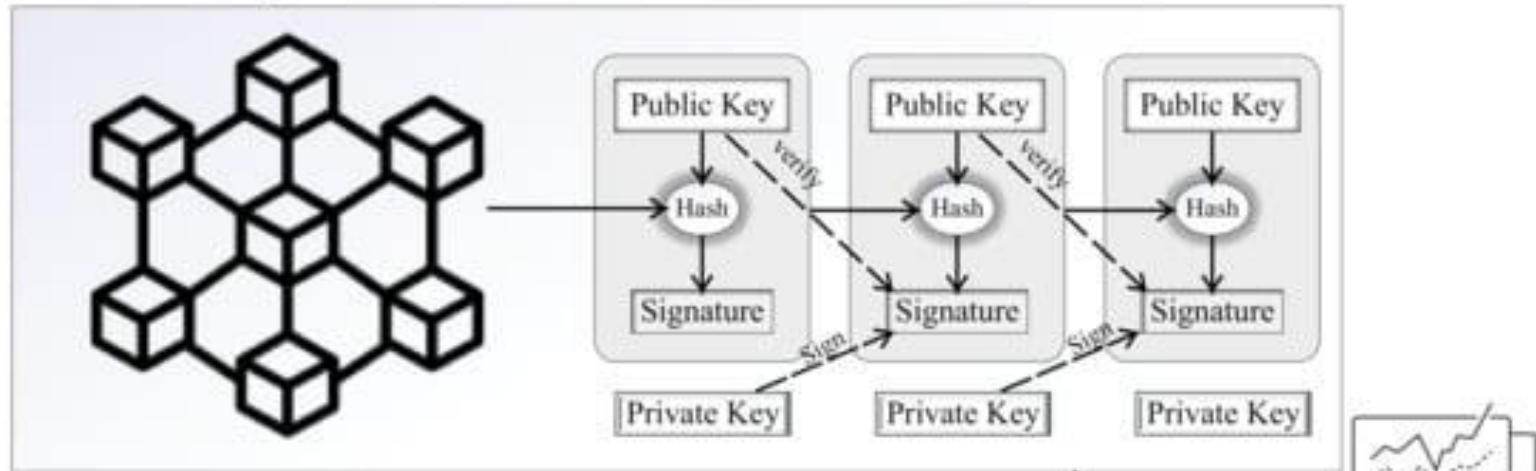
3 Alert, Record

- Alert stakeholders
- Flag and stop payments
- Record/Log Details

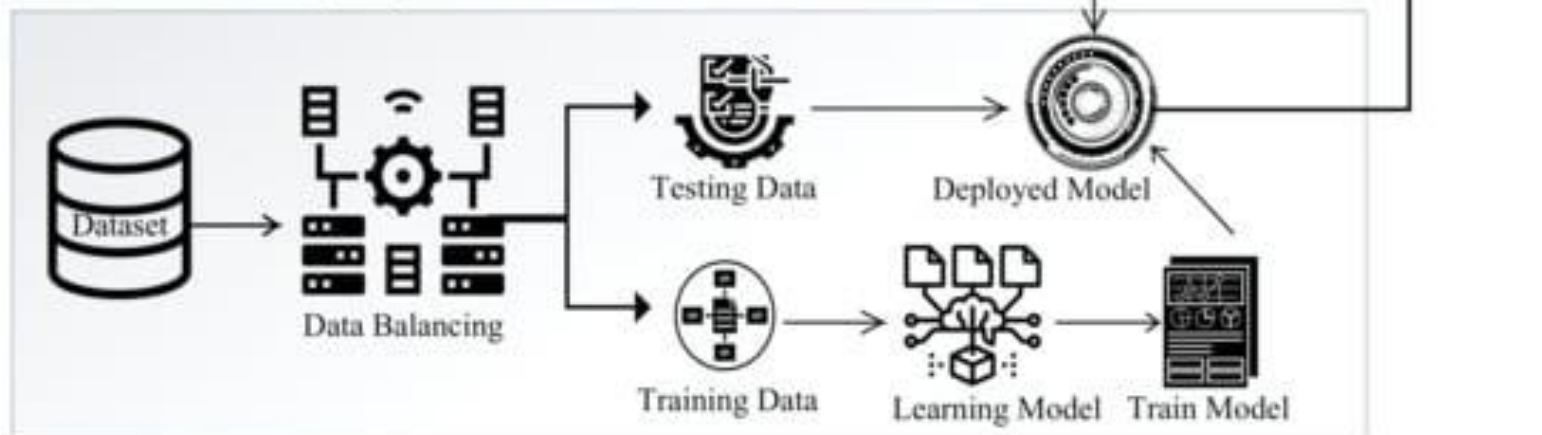


- Automated, quick and effective
- Improved accuracy
- Immutable logs and audit trail

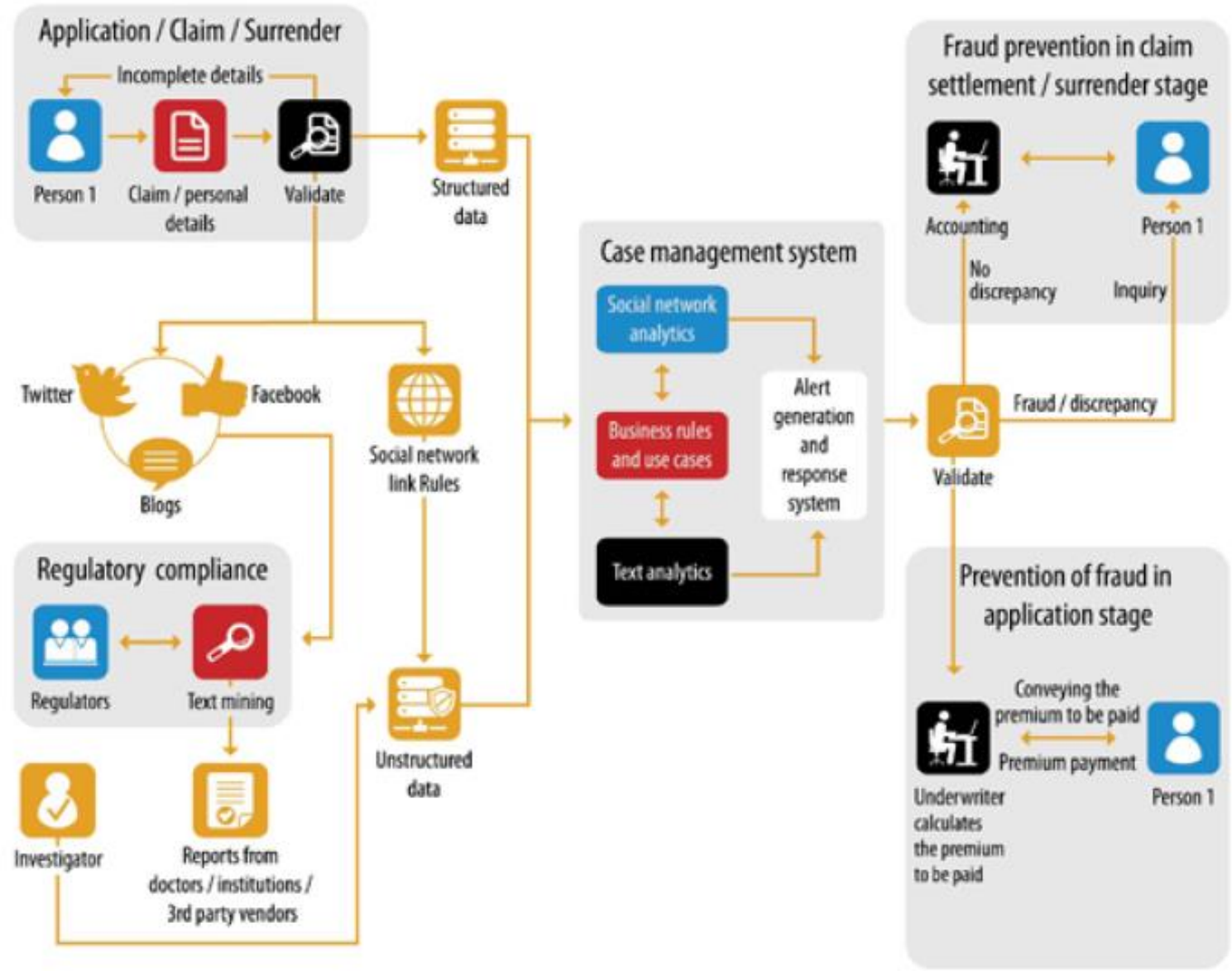
Blockchain Layer



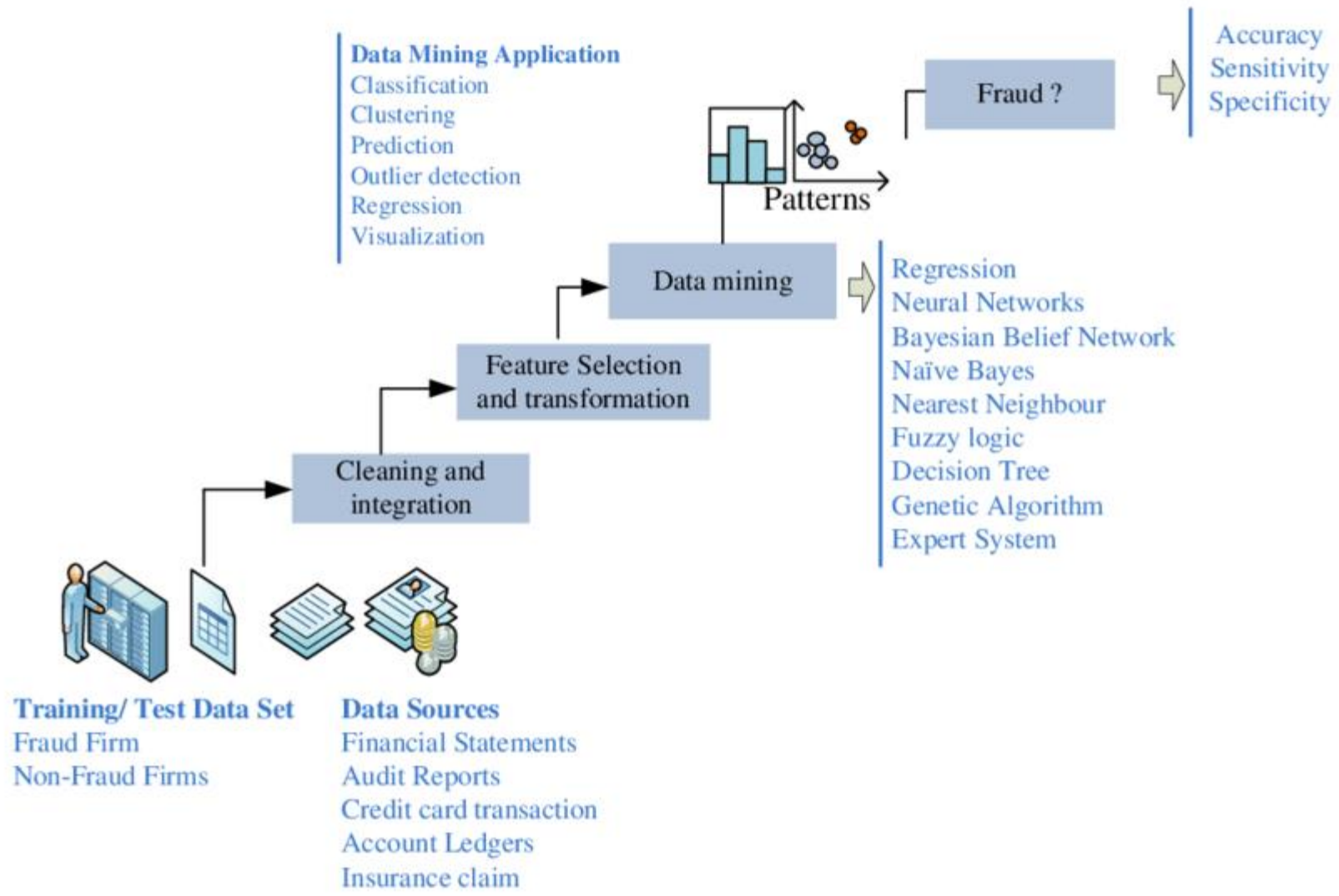
Machine Learning Layer



Implementing Analytics for Fraud Detection



Financial Statement Fraud – Text Analytics



Compliance Risk Assessment

