Blockchain

FTA Technology Conference

Pittsburgh, PA

August 9, 2016 (2:45 – 3:45)

Agenda

- Premise:
  - do we agree?
  - Consider these two ideas together …
- Five Fraudsters
- Blockchain via Bitcoin
- VAT
- Cigarettes

Do we agree ?

- Tax compliance systems are:
  - Highly centralized – single point of failure
  - Highly secure – are attacked and they attract attacks
  - Highly data driven – tax is naturally data-intensive
  - Concentrate power – susceptible to internal abuse
  - Slow – enforcement does not work in real-time
- Low level of Trust:
  - Among jurisdictions
  - Between the tax authority and the public

Blockchain is coming

- At the World Economic Forum more than 800 executive and technology experts were asked when a particular “tipping point” would be reached …
- When would we see a government collect tax with blockchain ?
- ANSWER: 2023
- 73% expected “by at least 2025”.
- Which tax?
- Which country?

Five Fraudsters

Who took advantage of tax systems

Could they be stopped in real-time with BLOCKCHAIN ?

Funded by Tax Fraud

Hizballah Sheikh
Muhammad Hussein
$20 million/ 4 yr.
RST (Michigan)

Osama bin Laden
€1.5 billion/ 1 yr.
VAT (Italy)

Samir Azizi €61,104,368/ 1 yr.

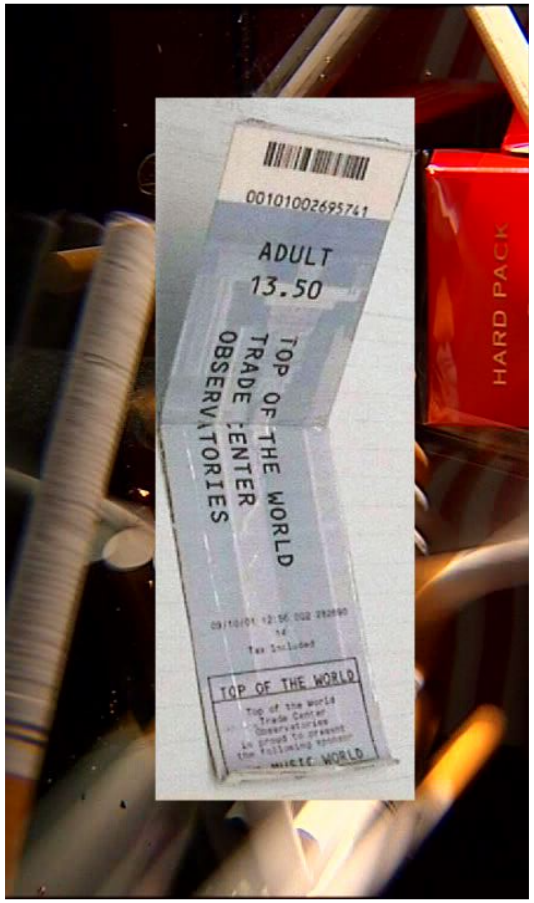
Germany

Taha “Saleh” Mutaher

20,000 cigarette ctn/wk = $65m (16 arrested)

North Carolina to NYC

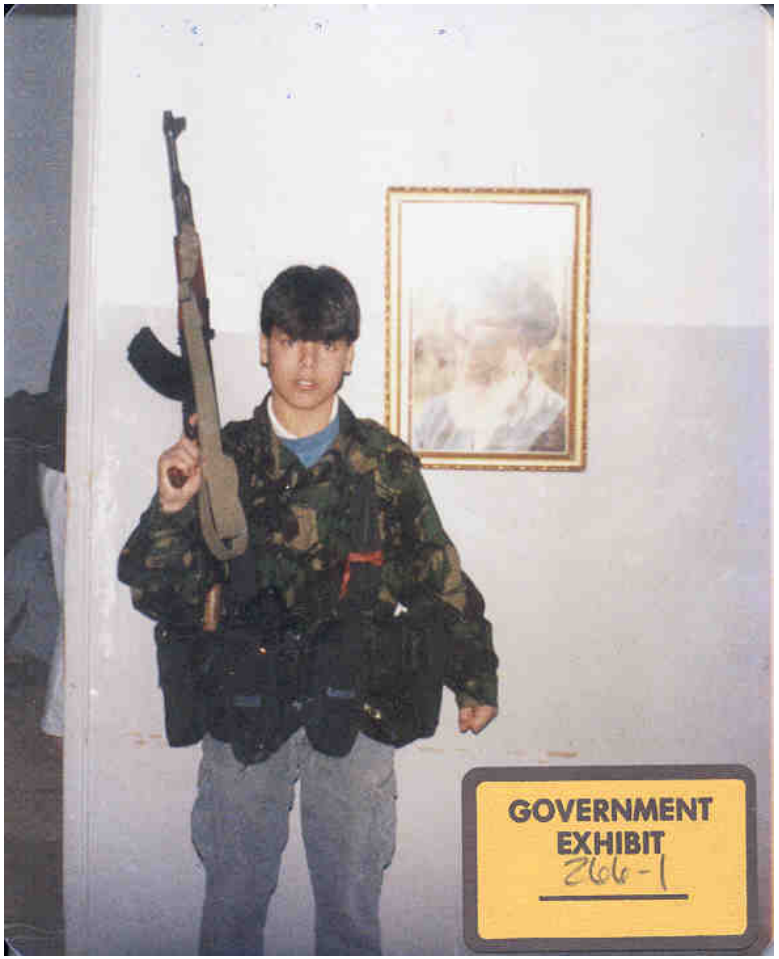
September 10, 2001 **20 hours before** **September 11, 2011**



Mohamad Youssef Hammoud

30 years (jury = 155 yrs) – $8m cigarette smuggler – 37 yr old

Virginia to Michigan



Blockchain/ Bitcoin

What is Blockchain / What is Bitcoin

- Distributive Ledger Technology & an App
- It all began with Bitcoin (2008) [cryptography mail list]
  - Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system* (2008) available at: https://bitcoin.org/bitcoin.pdf
  - Previous digital currency (1996)
    - E-GOLD
    - Liberty Reserve

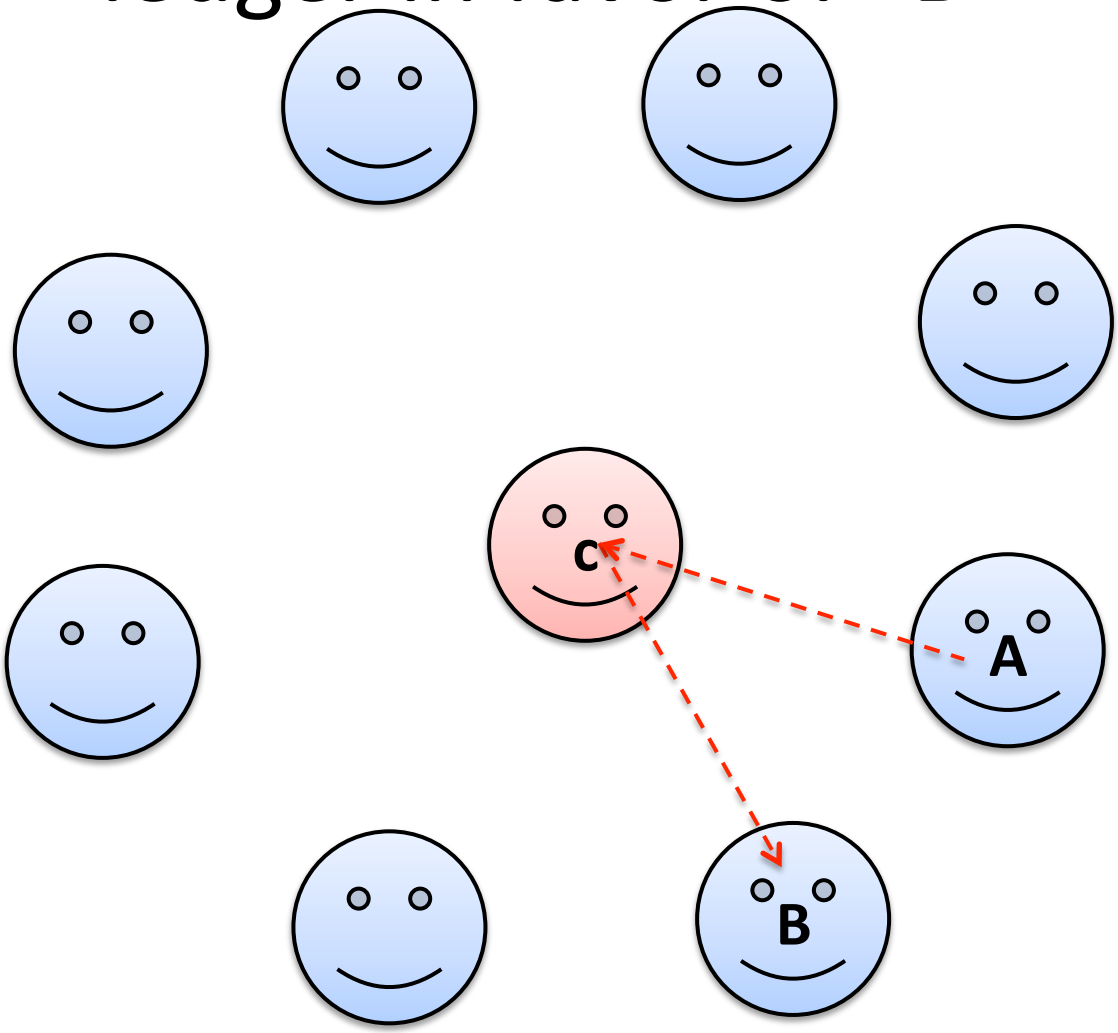
Billions of dollars
Buy a balance in
oz. gold or
Liberty dollars

  - 2001 Patriot Act tightens "Money Services Business
  - 2013 both are shut down (money laundering)

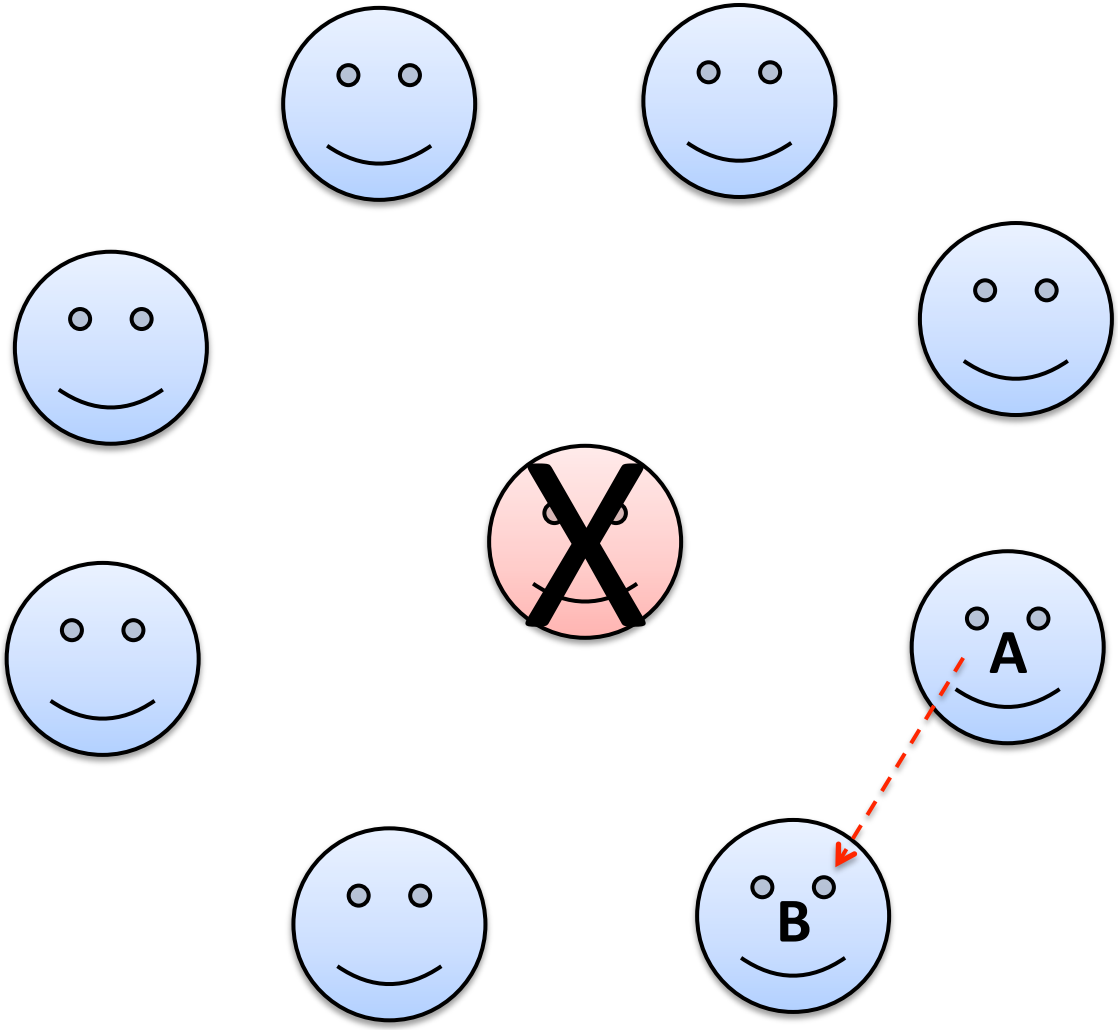
Digital Currency (before Bitcoin)

- Prior to Bitcoin all digital currencies had central control [just like a traditional finance system]
  - A could not pay B without relying on an intermediary
- For “A” to pay “B”
  - “A” asks the center to update the general ledger in favor of “B”
  - “A” must trust that center will do it faithfully
  - The problem for Satoshi Nakamoto was the system puts too much power (and money) in the hands of the central authority

“A” asks “C” to update the central ledger in favor of “B”



Satoshi Nakamoto:
“A” sends X-amount to “B”



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Problems with Centralized Systems

- A centralized ledger of balances is controlled by single [trusted] entity, but the system….
  - Has a single point of failure
    - Government could shut it down (e-GOLD; Liberty Reserve)
    - Disgruntled employee could do the same
    - A cleaning person's accident could do it too <joke>
  - Is prone to corruption
    - Embezzlement
  - Is inherently insecure
    - Hackers
  - But it is designed to stop Double Spending

Double Spending

- Biggest problem in a decentralized digital cash system:
  - How can you prevent the same balances in a ledger from being spent twice without resorting to a central authority ?
  - Essentially the ledger is all data (it can be manipulated) … must have a “trusted party,” right?
- Byzantine Generals Problem

Bitcoin/ Blockchain

This is all about "consensus"

- Every participant has a record of every transaction that has ever happened
  - Example: 10 btc to Hal Finney from Satoshi Nakamoto (1-12-2009)
  - Any participant can use computing resources to work a math problem – problem is designed for the network to produce a correct answer once every 10 minutes – Massive brute force guessing
  - In the meantime people are using the network to exchange coins, -- if you solve the problem above you get the right to collect all transactions into a block and submit them for a bitcoin reward.
  - Every node will get a copy of the block and decide if it is valid or not.
  - Validating = comparing the block w/ list of transactions received.
  - If it is fine, add it to the chain, and begin working on the next block
- Bitcoin Consensus = Proof of Work
- There are many others:
  - Proof of Stake;
  - Proof of Identity;
  - Proof of Elapsed Time (POET)
  - Quorum Voting (QV)

} Developed by INTEL for the Sawtooth Lake blockchain platform

Proof of Work

- First:
  - Collect unconfirmed transactions (maybe 1,000)
  - Perform “consensus rule validation” on each
    - List of 30-40 rules for each transaction
    - List of 30-40 rules for each block.
- Second:
  - Take the header of the previous block
  - Plus a number (called a “nonce”) a 32-bit (4 byte) field whose value is set so that the hash of the block will contain a run of zeros.
  - Use SHA256 …. 10 minutes …. Perform 500 quadrillion hashes per second … find a number less than the target
- Third:
  - Incur costs … announce to world you have the next block …wait for validation (other nodes will check the “consensus validation”)
- Fourth:
  - get a reward (new Bitcoin)

Re-cap – What is Bitcoin ?

- Bitcoin is:
  - First real cryptocurrency
  - Using a peer-to-peer network
  - Creating a decentralized ledger
  - Solving the “double spend” problem

Re-cap – What is Blockchain ?

- Blockchain:
  - Is a decentralized database (ledger) with network enforced processes for updating the database.
  - Is a general purpose technology that can be applied to disrupt (i.e., provide exciting computer-based alternatives to) any centralized system that coordinates valuable information
  - Is secure even in the presence of powerful 3rd parties who would like to prevent users from participating
  - Is especially applicable to data intensive, rather than capital intensive industries/ activities.

Blockchain "takeaways"

- High transparency
  - All participants can see all transactions (but encrypted)
- High resilience/ availability
  - No central point to bring the network down (censorship resistant)
- High trust/ security (trust the code)
  - Network enforced properties – cannot hack the network
- High efficiency/ Low cost
  - Compared to centralized systems which have a lot of intermediaries that need to be paid:
    - Moore's Law: cost of processing a bit (half in 18 mo.)
    - Kryder's Law: cost of digital storage (half in 12 months)
    - Nielson's Law: cost of bandwidth (half in 24 months(

Data Intensive Industries

- Finance
  - Cash/bank deposits … inflation [limited currency]; slow transfers [5x faster]; expensive transfers [Western Union 10% fee]; ease of seizure [need private key]; difficulty of micropayments [easy])
  - Provability of reserves … no Ponzi schemes (Madoff)
  - Trustless P2P markets … banks & market manipulation
- Gaming
  - Provably fair gambling … [Bitzino.com – verifiable card game], [Chance Casino – full casino fully virtual]
- Communications
  - Censorship resistant … [Bitmessage … P2P decentralized encrypted message mimics Bitcoin … anonymous & broadcast to whole network, with proof-of-work]; Domain Name Service – Internet ICANN can pull domain names (WikiLeaks) & internet could be attacked here at Root DNS Servers to take down the net… NameCoin (.bit)]
  - P2P cloud – because the cloud is highly centralized … could be hacked (STORJ.IO allows you to share excess hard-drive capacity for capacity in the cloud … paid in STORJ coins) … files are cut into small chunks and spread across the network … no admin privileges … only you have keys)
  - Share economy – Uber; Lyft; AirBNB [ripe for disruption, because the value in not in the technology, but the network – see LaZooz… a decentralized Uber – a decentralized autonomous network; not a taxi like Uber, but make use of rides already underway in exchange for La'Zooz Tokins earned like Bitcoin by giving others' rides]
- Future
  - P2P energy network (solar bought & sold) – rate rigging & over financialization increasing prices.
  - P2P Communications networks (alternative to the Internet) … based on rewards for sharing bandwidth
  - P2P Logistics Networks delivery technology (drones, etc.)
  - Backbone to a future IoT (see IBM) building chips for the toaster & refrigerator with shared bandwidth paid in micro bitcoins

- **No one mentions taxation**

Two Kinds of Blockchain

Distinguished by the consensus mechanism

- Permissionless – public or un-restricted
  - Bitcoin
  - Bitzino
  - LaZooz
  - Bitmessage
- Permissioned – private or restricted
  - European Central Bank
  - Bank of Canada

VAT

In the EU MTIC fraud is a

€100 billion/yr

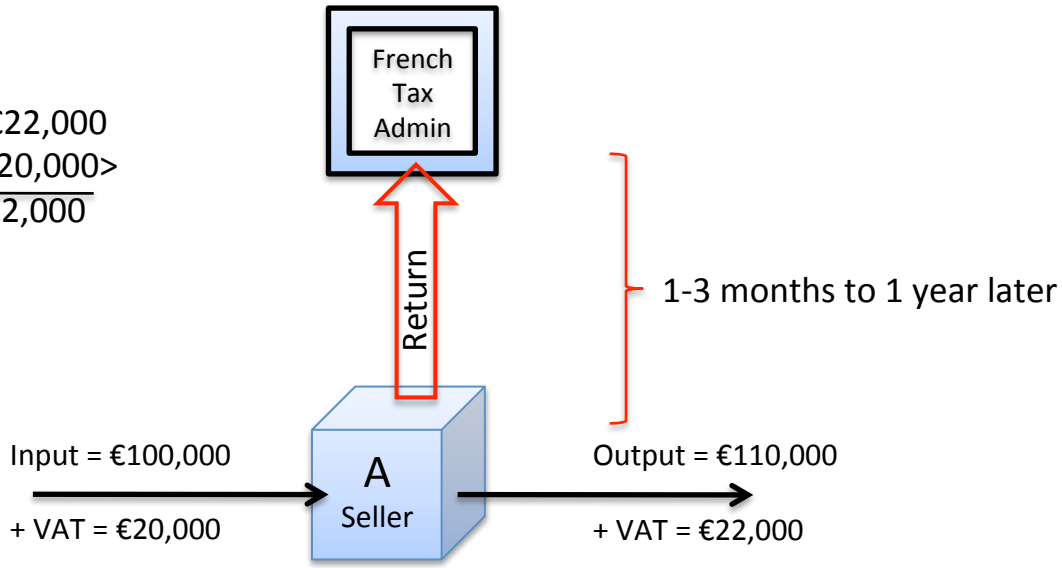
problem

The Problem

- Missing Traders
  - MTIC fraud
  - MTEC fraud
  - Bankruptcy
- Estimated losses
  - €100 billion fraud (annually) Europol, *SOCTA (Serious and Organized Crime Threat Assessment)* March 2013.
  - €193 billion (in 2011) $258 billion VAT gap *Study to Quantify and Analyze the VAT Gap in the 27 Member States* (TAXUD/2012/DE/316) (July 2013).

VAT

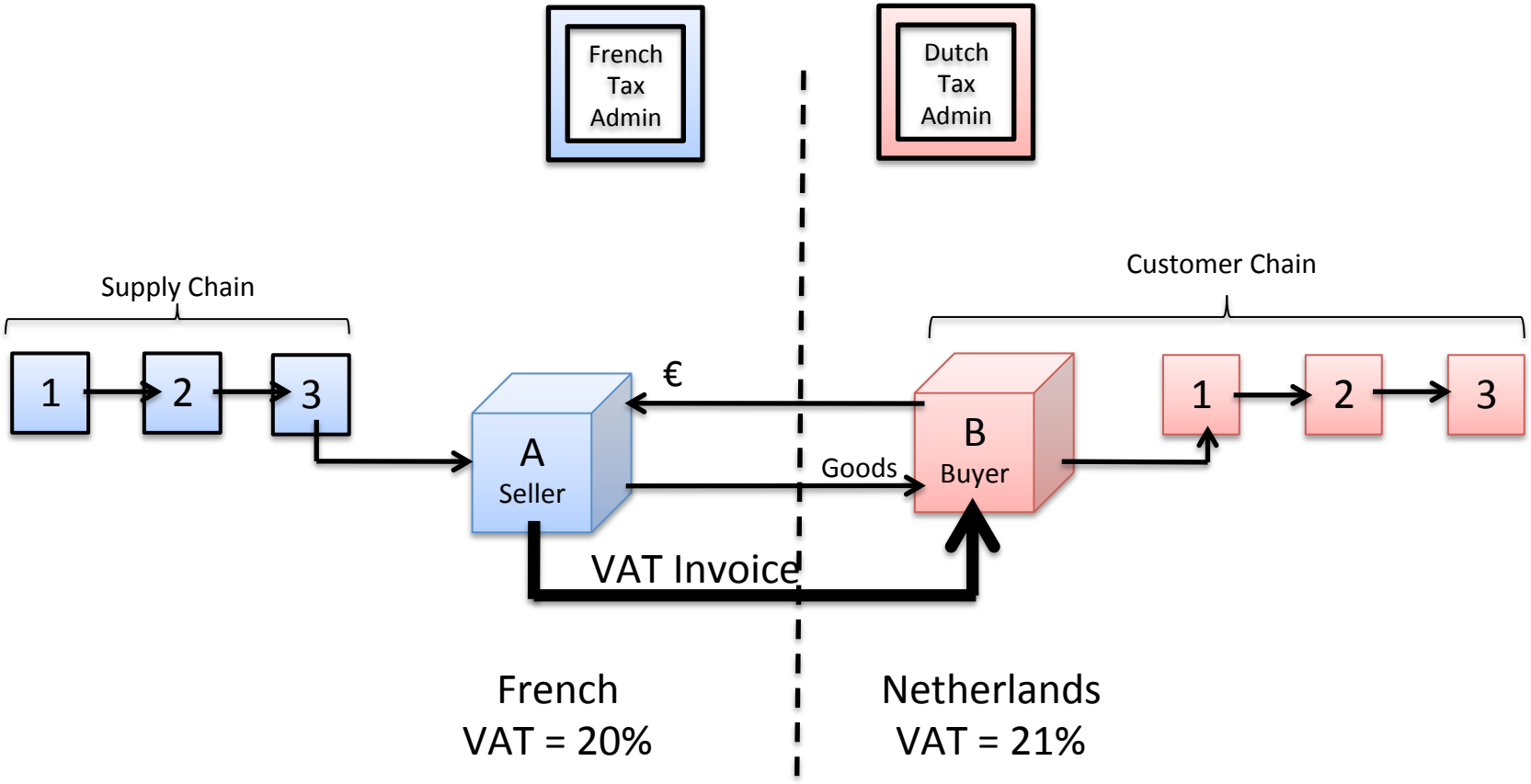
Output VAT Collected ….€22,000
Input VAT paid ……..<€20,000>
Net……..€2,000



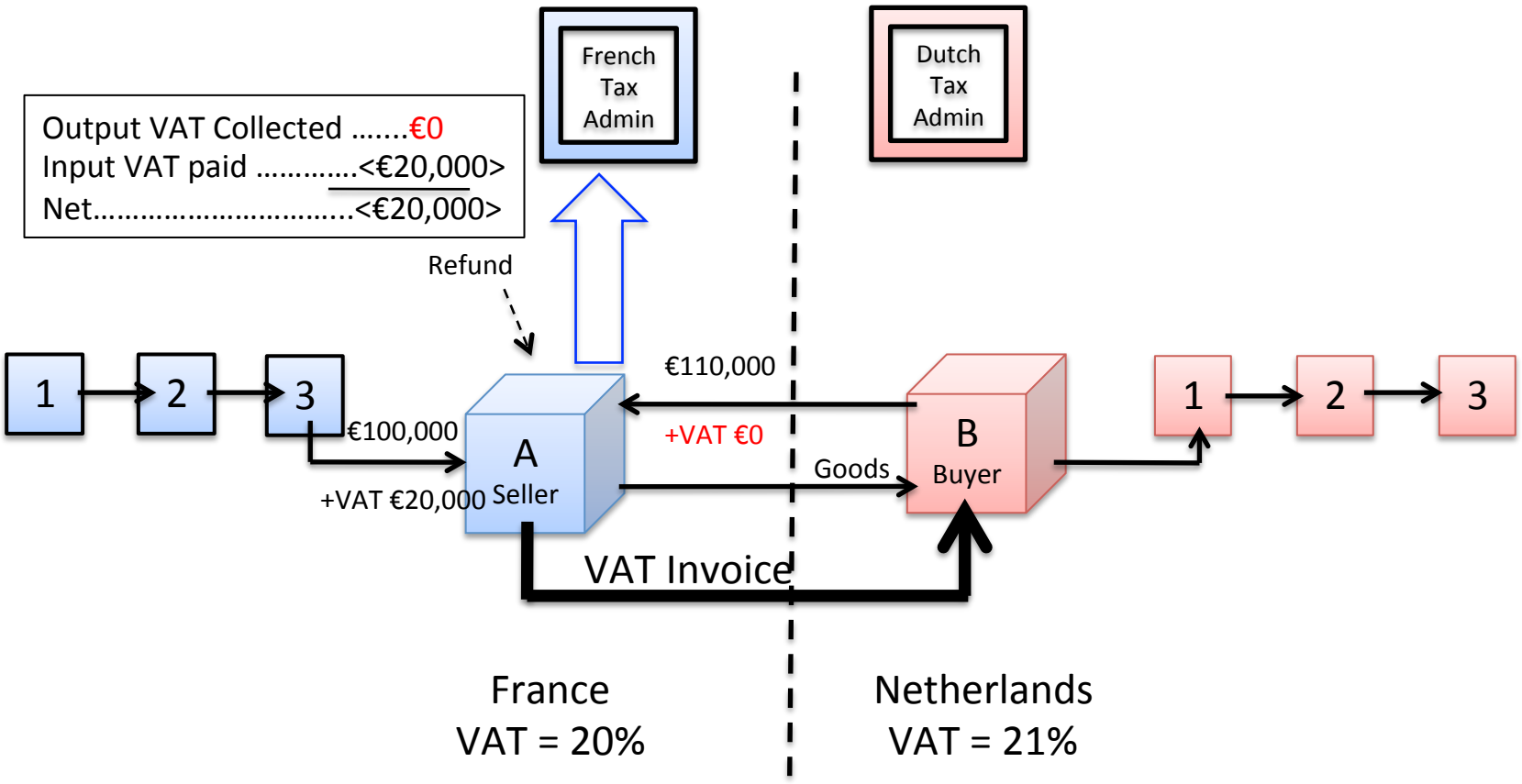
France
VAT = 20%

Notice: Value added by "A" is €10,000 and rate is 20%, so net due is 20% x €10,000 = €2,000

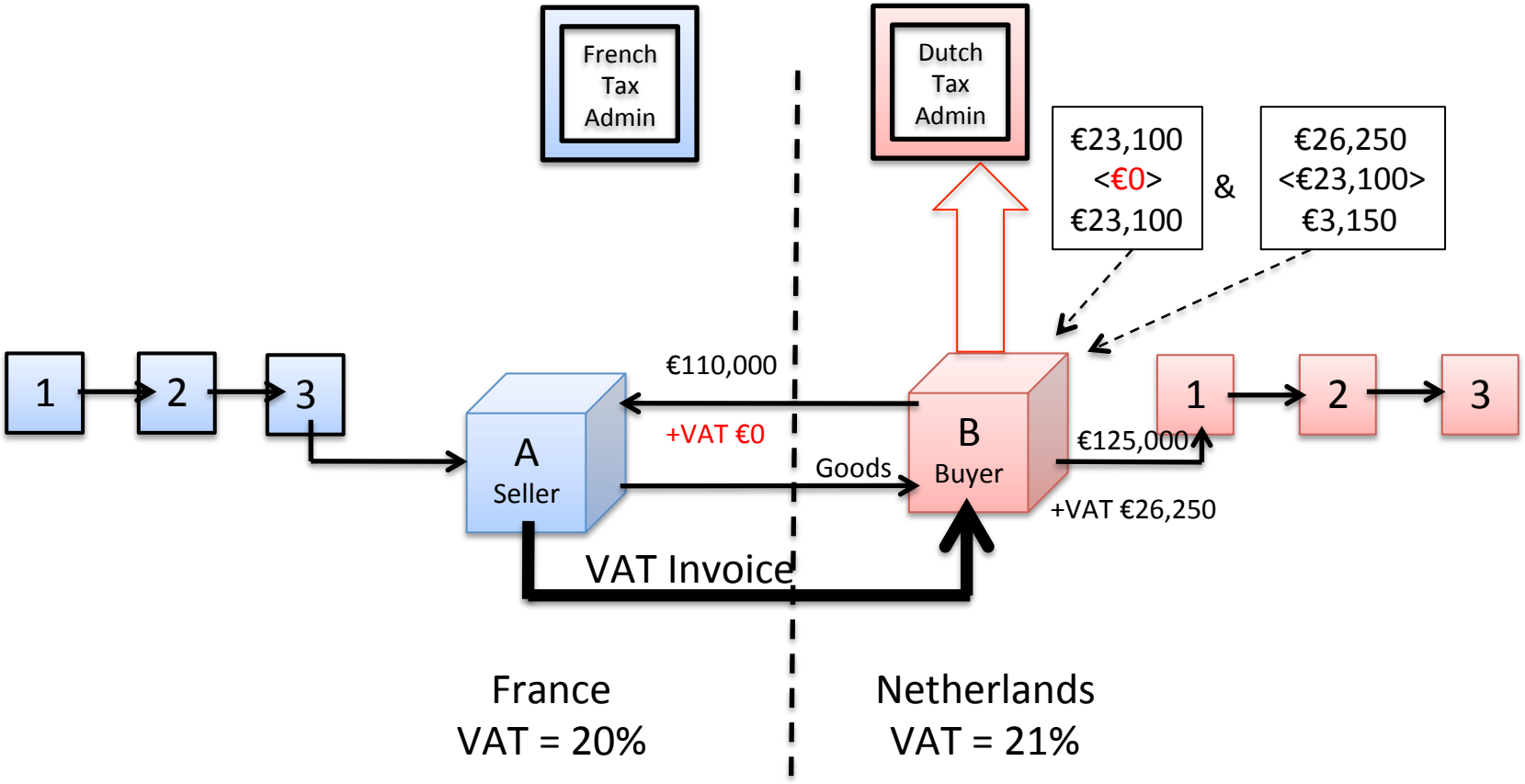
Cross Border 1/4



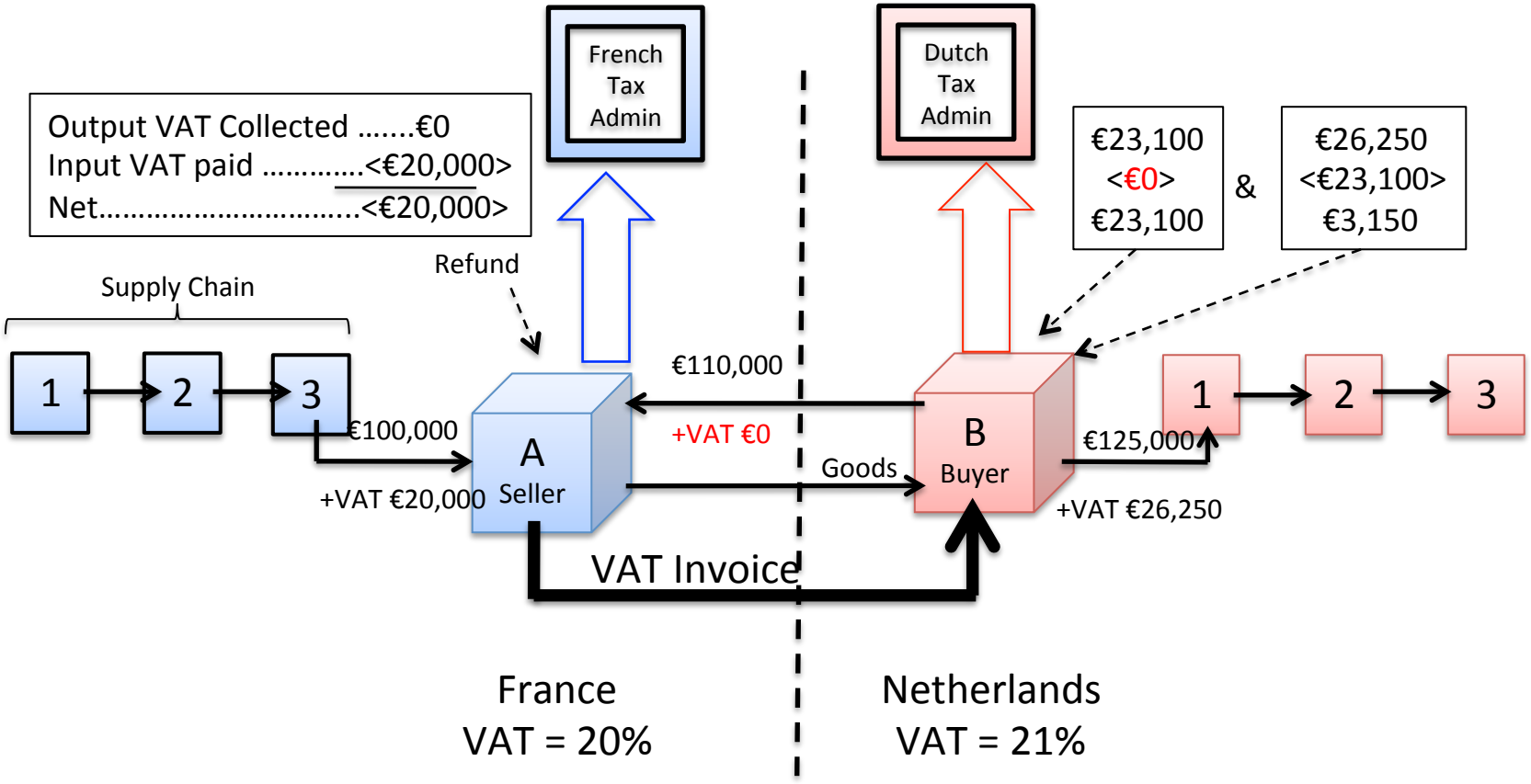
Cross Border 2/4



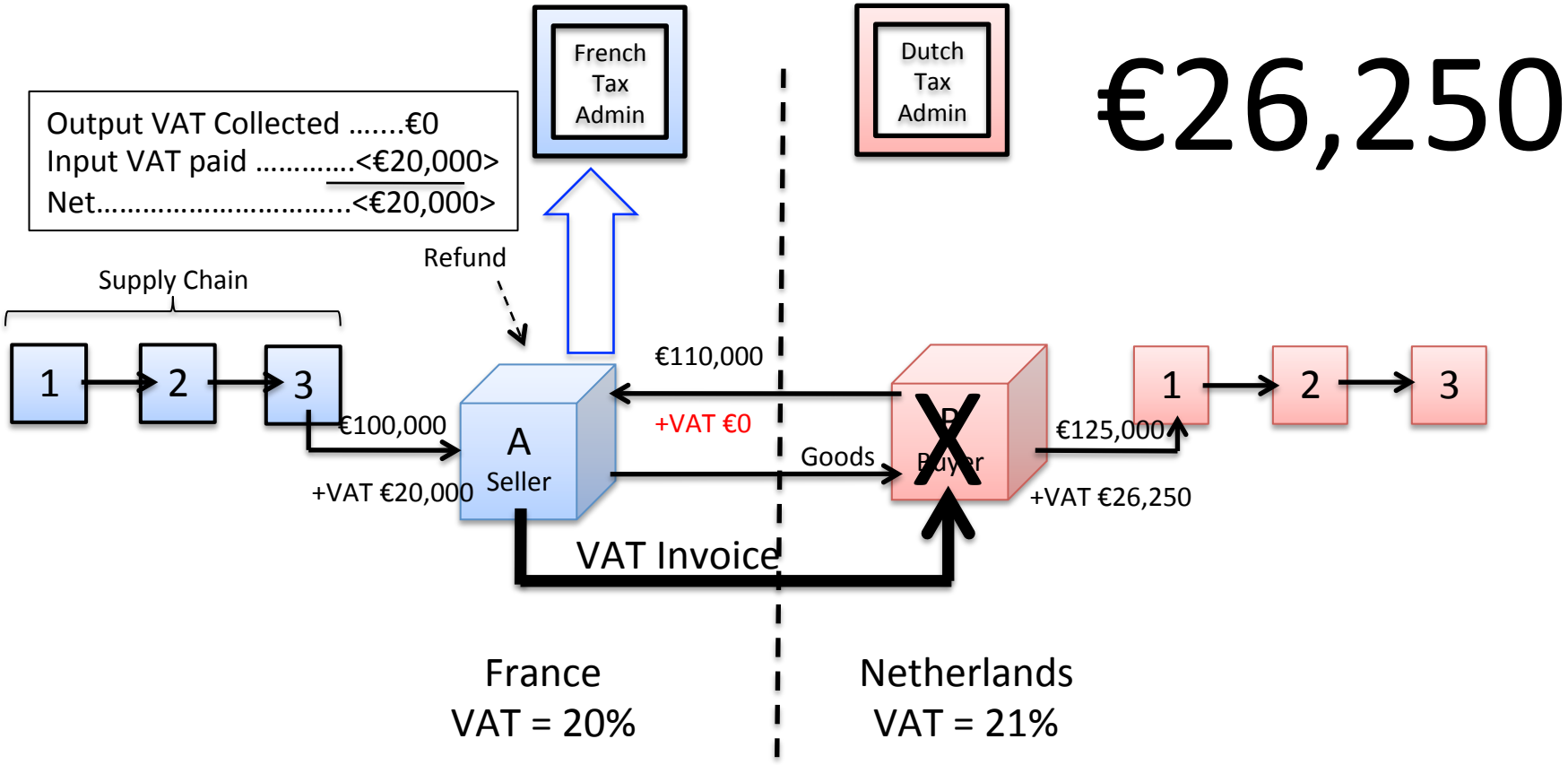
Cross Border 3/4



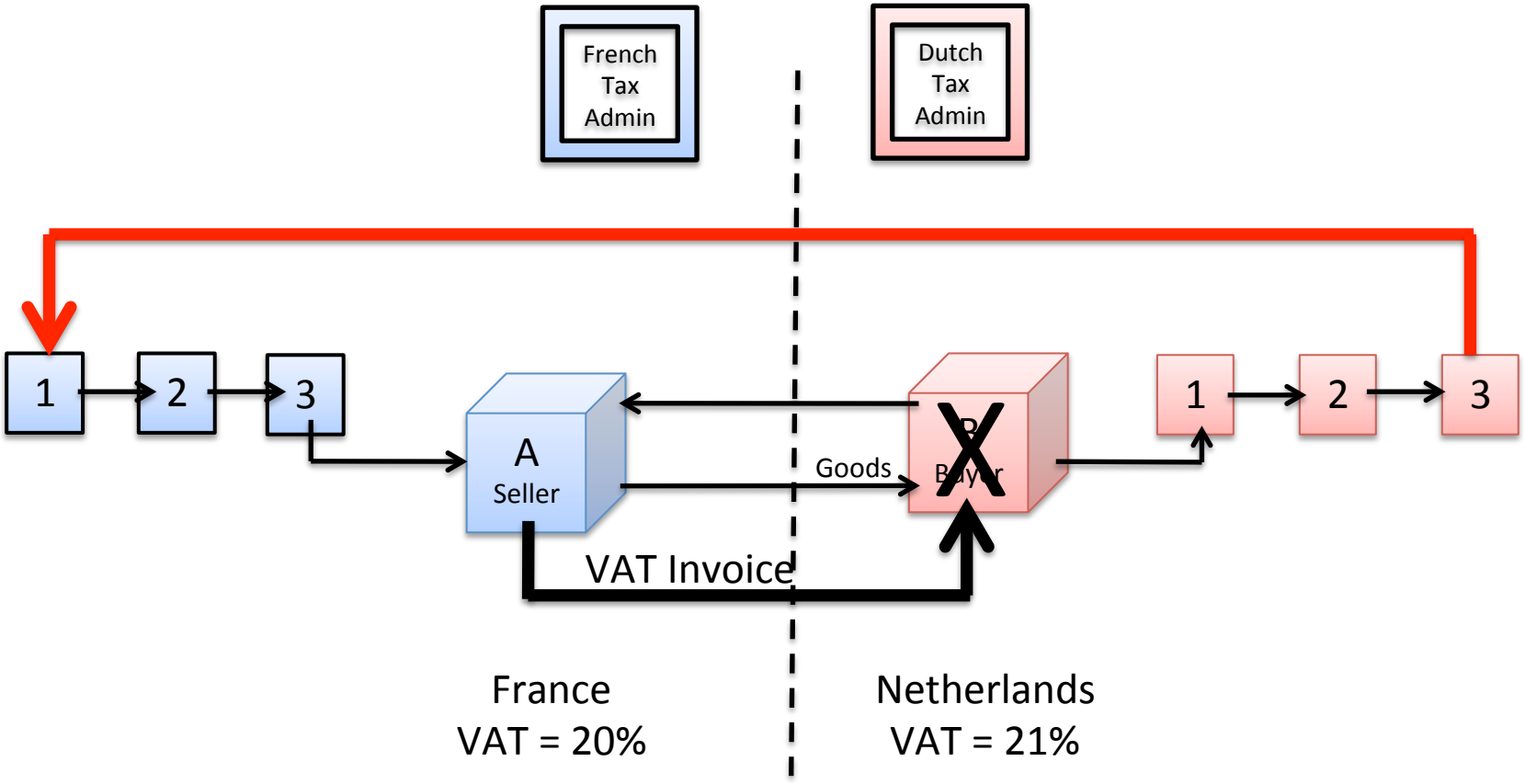
Cross Border 4/4



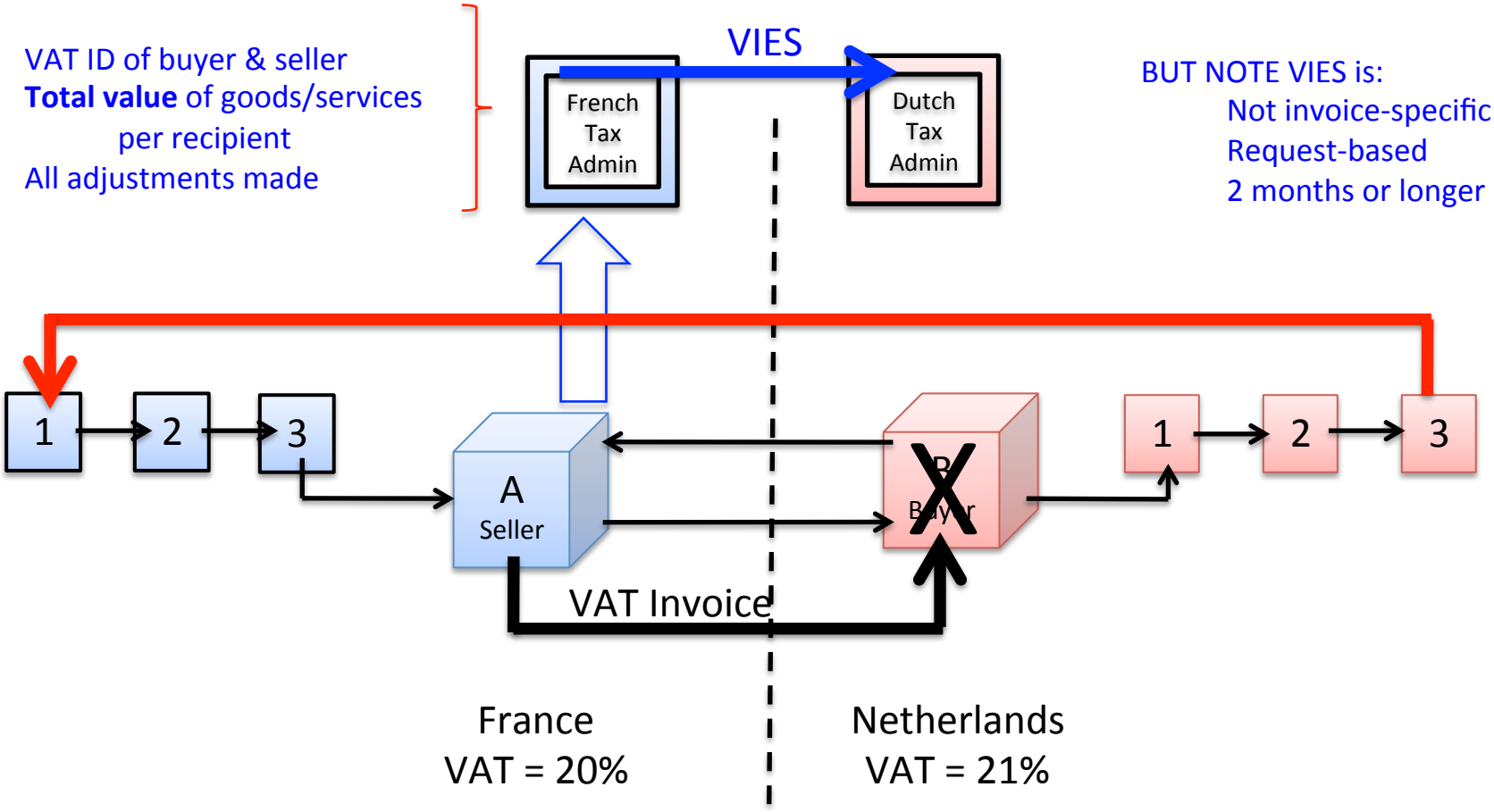
MTIC


French Tax Admin
Dutch Tax Admin
€26,250
Output VAT Collected €0
Input VAT paid .....<€20,000>
Net.....<€20,000>
Refund
Supply Chain
1
2
3
€100,000
+VAT €20,000
A
Seller
€110,000
+VAT €0
Goods
B
Buyer
€125,000
+VAT €26,250
1
2
3
VAT Invoice
France
VAT = 20%
Netherlands
VAT = 21%

Carousel


French Tax Admin
Dutch Tax Admin
1
2
3
A
Seller
Goods
B
Buyer
1
2
3
VAT Invoice
France
VAT = 20%
Netherlands
VAT = 21%

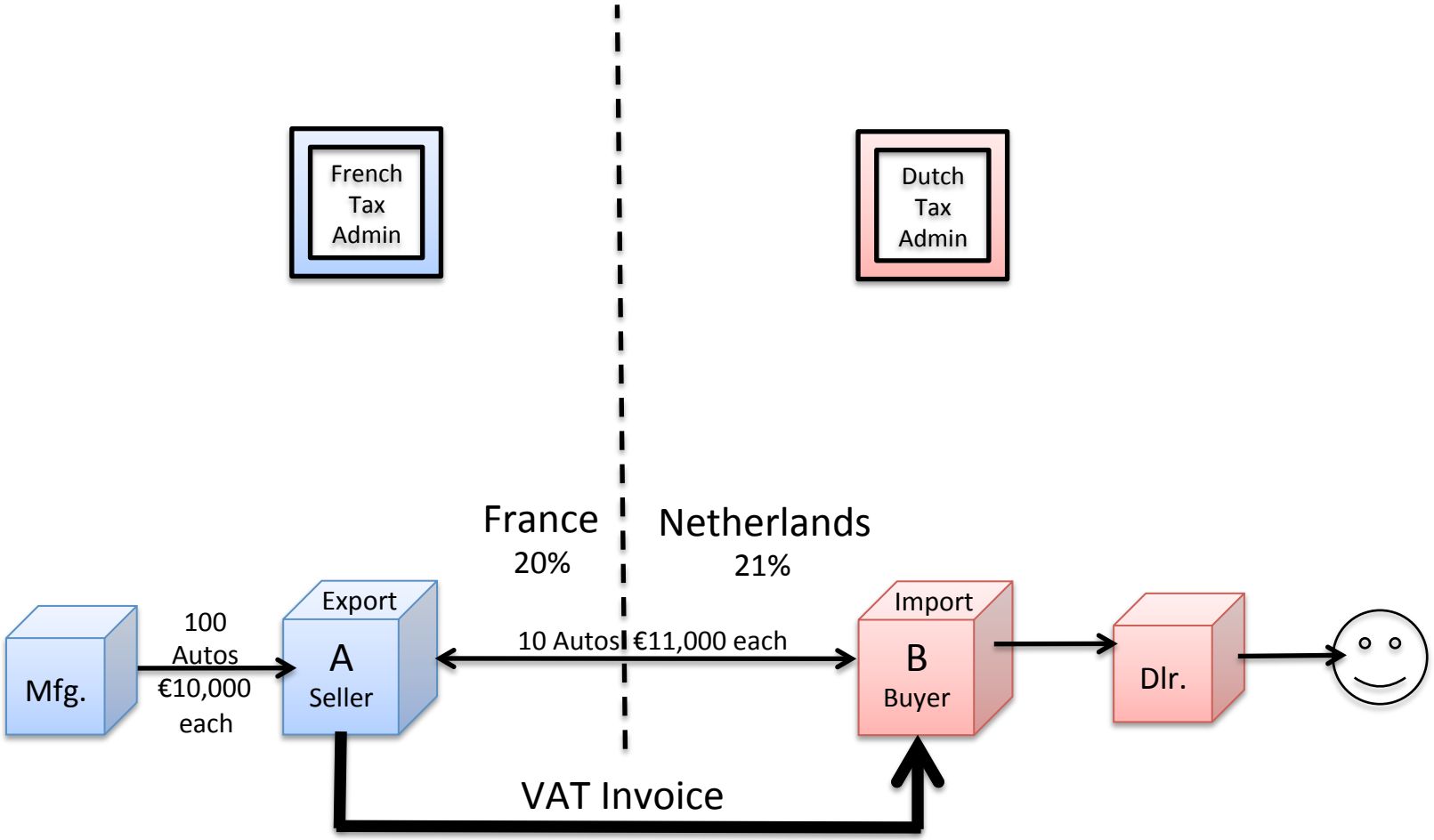
VIES


VAT ID of buyer & seller
Total value of goods/services per recipient
All adjustments made
VIES
French Tax Admin
Dutch Tax Admin
BUT NOTE VIES is:
Not invoice-specific
Request-based
2 months or longer
1
2
3
A
Seller
B
Buyer
1
2
3
VAT Invoice
France
VAT = 20%
Netherlands
VAT = 21%

Solution(s)

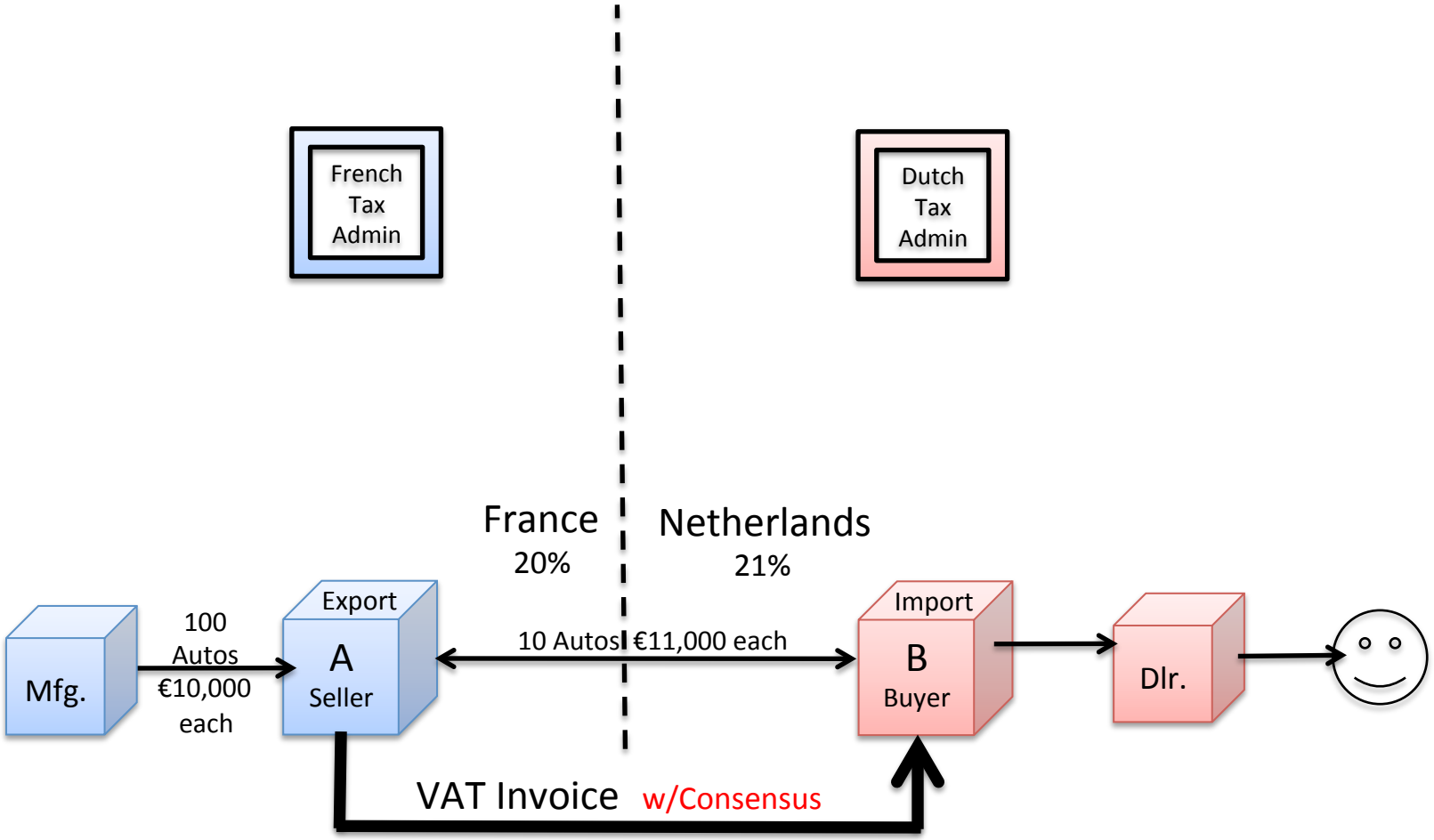
- Central collection of B2C data:
  - Quebec (CGI), Ontario, Sweden (R/I), Germany (INSIKA),
- Central collection extended to B2B – DICE
  - Real-time, encrypted, shared public key (cross-border ?)
  - Rwanda (DTI); Ceará, Brazil (SmartCloud Inc.); Croatia; GCC; EAC
  - Modeled on Brazilian (federal) *SPED*
- Decentralized distributed ledger – Blockchain DICE
  - Proposal (only) … so far
  - Least expensive; most secure; high trust
  - Permissioned blockchain
    - Follow European Central Bank; Bank of Canada …

VAT Blockchain with 75% consensus threshold [1/7]

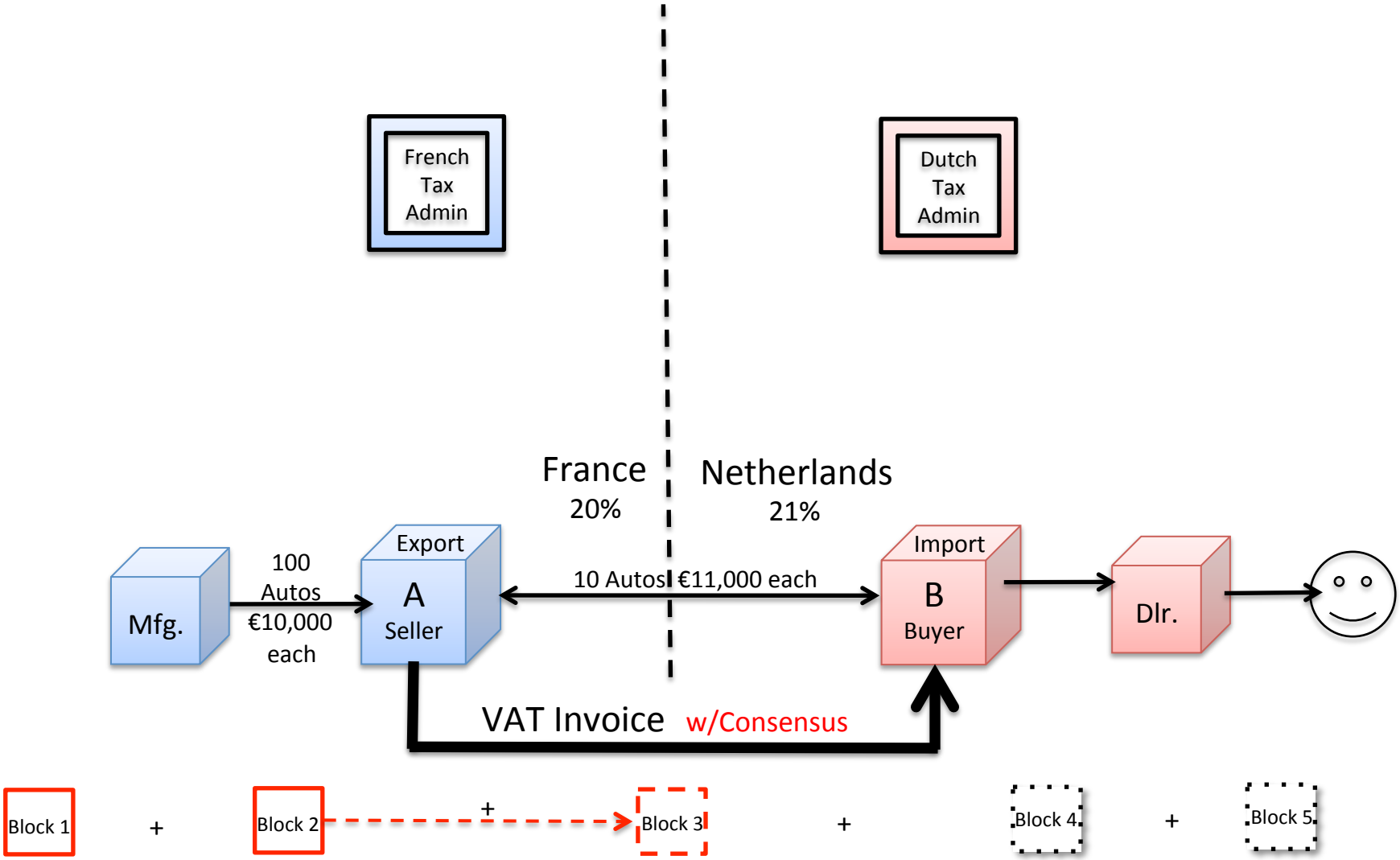


VAT Blockchain with 75% consensus threshold [2/7]

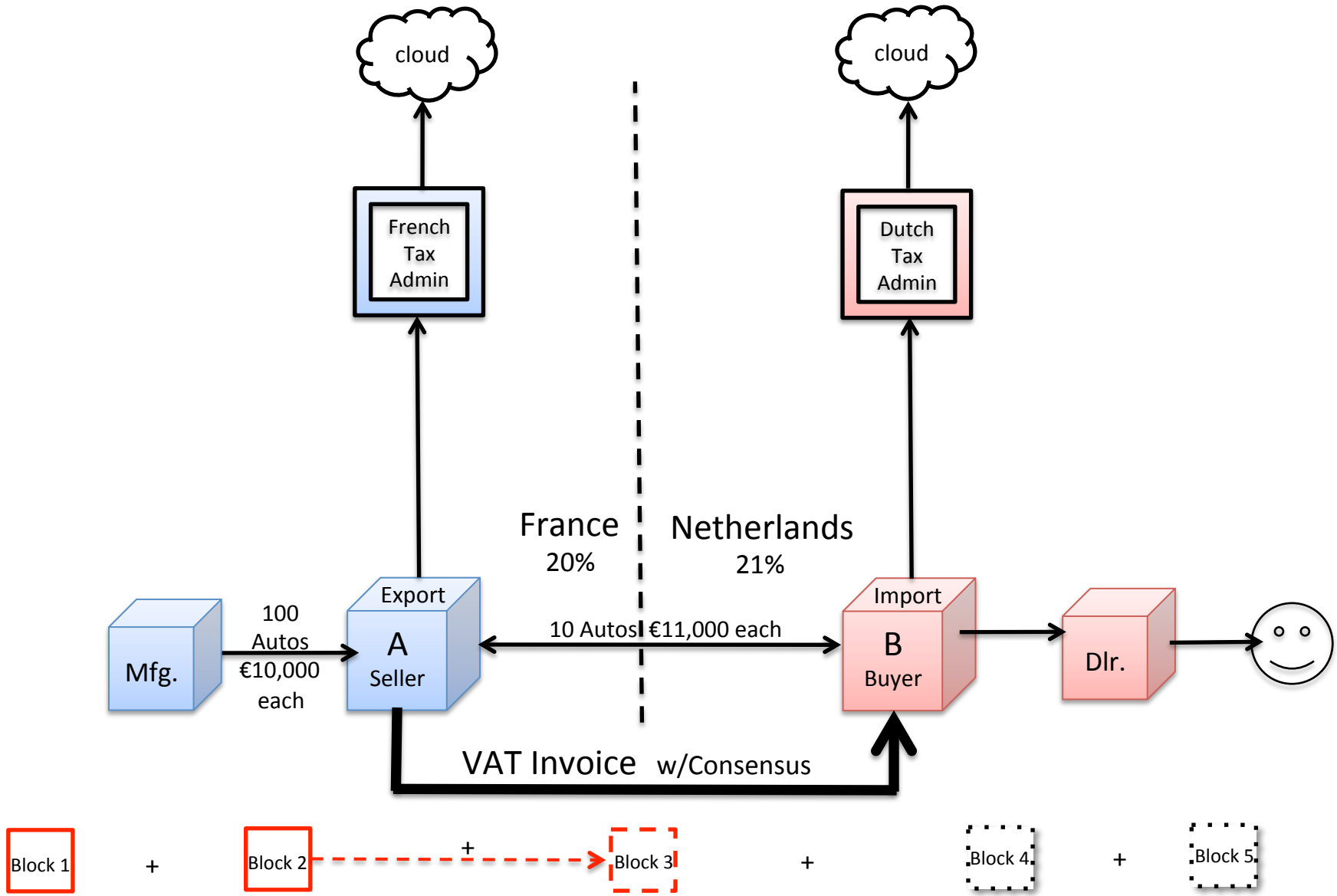
Not just a VAT Invoice, we want a VAT Invoice with CONSENSUS



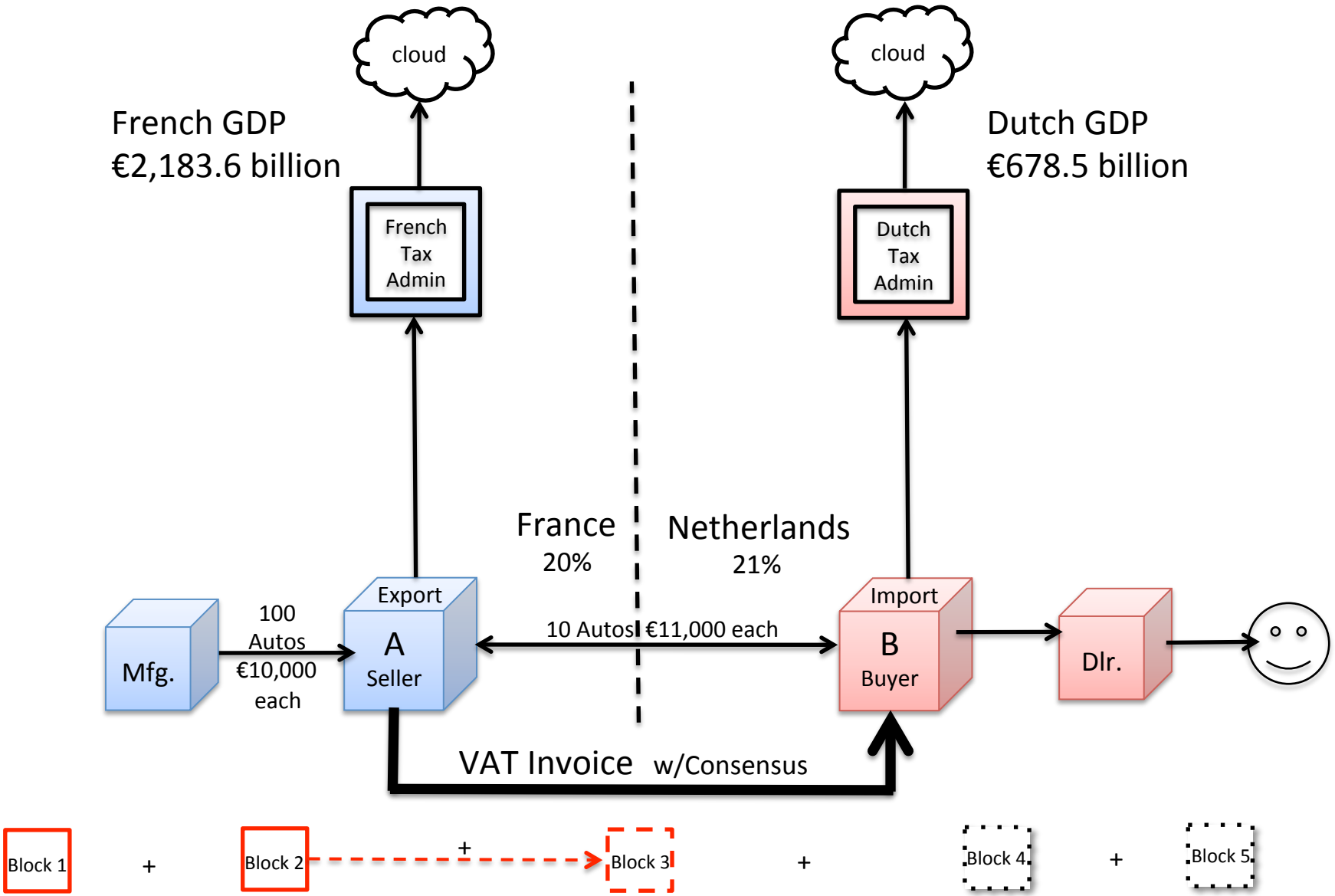
VAT Blockchain with 75% consensus threshold [3/7]



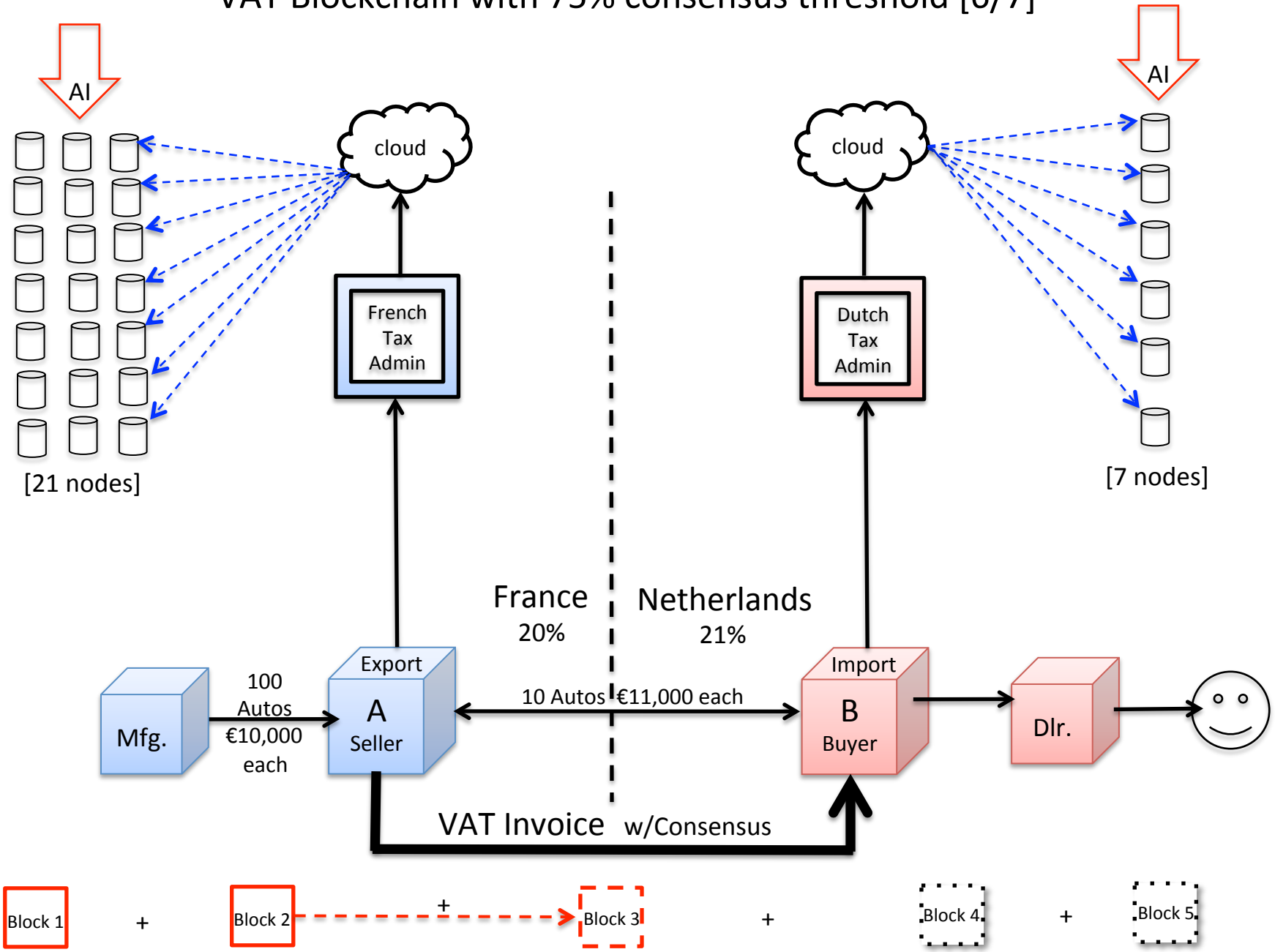
VAT Blockchain with 75% consensus threshold [4/7]



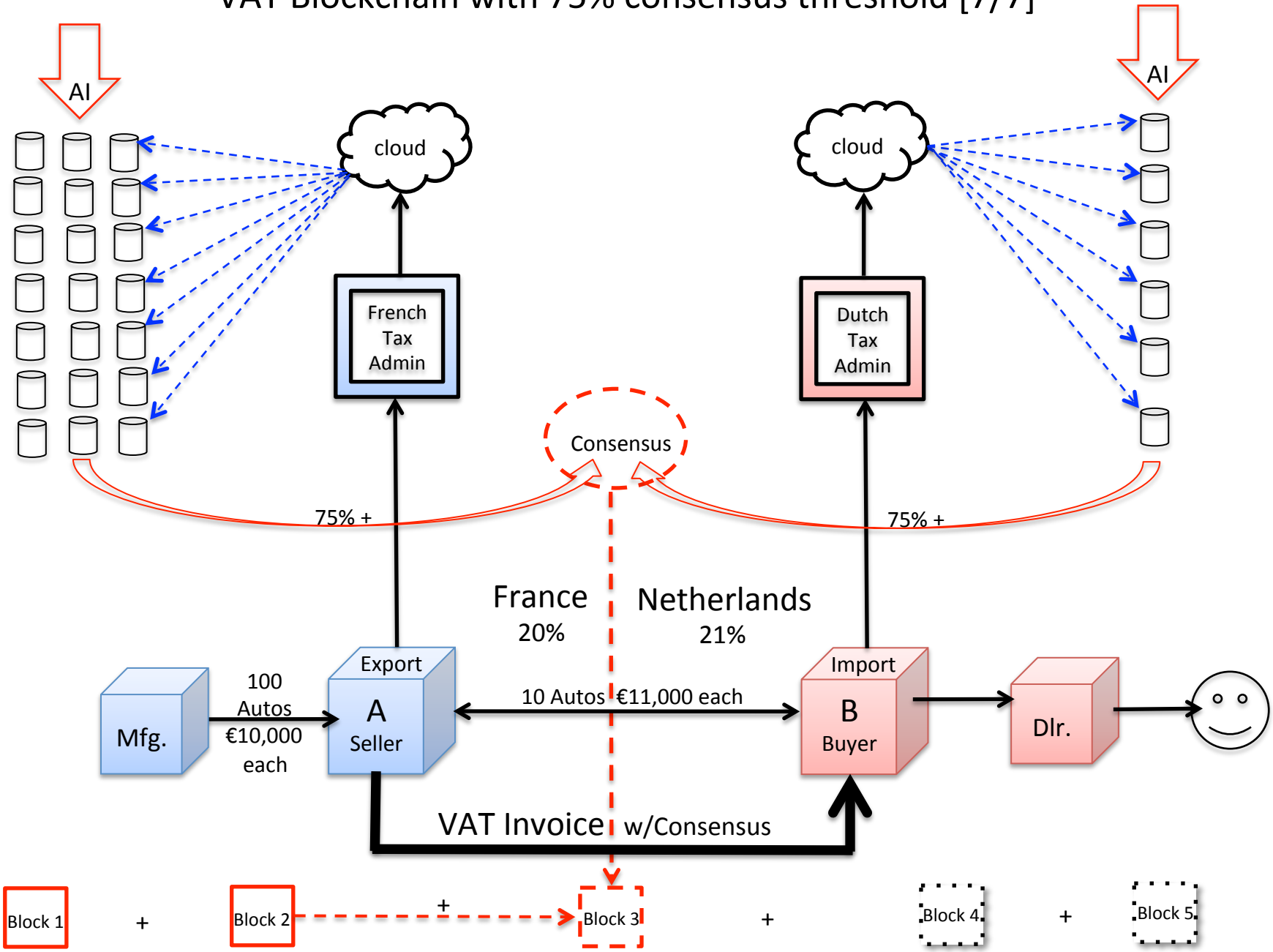
VAT Blockchain with 75% consensus threshold [5/7]



VAT Blockchain with 75% consensus threshold [6/7]



VAT Blockchain with 75% consensus threshold [7/7]



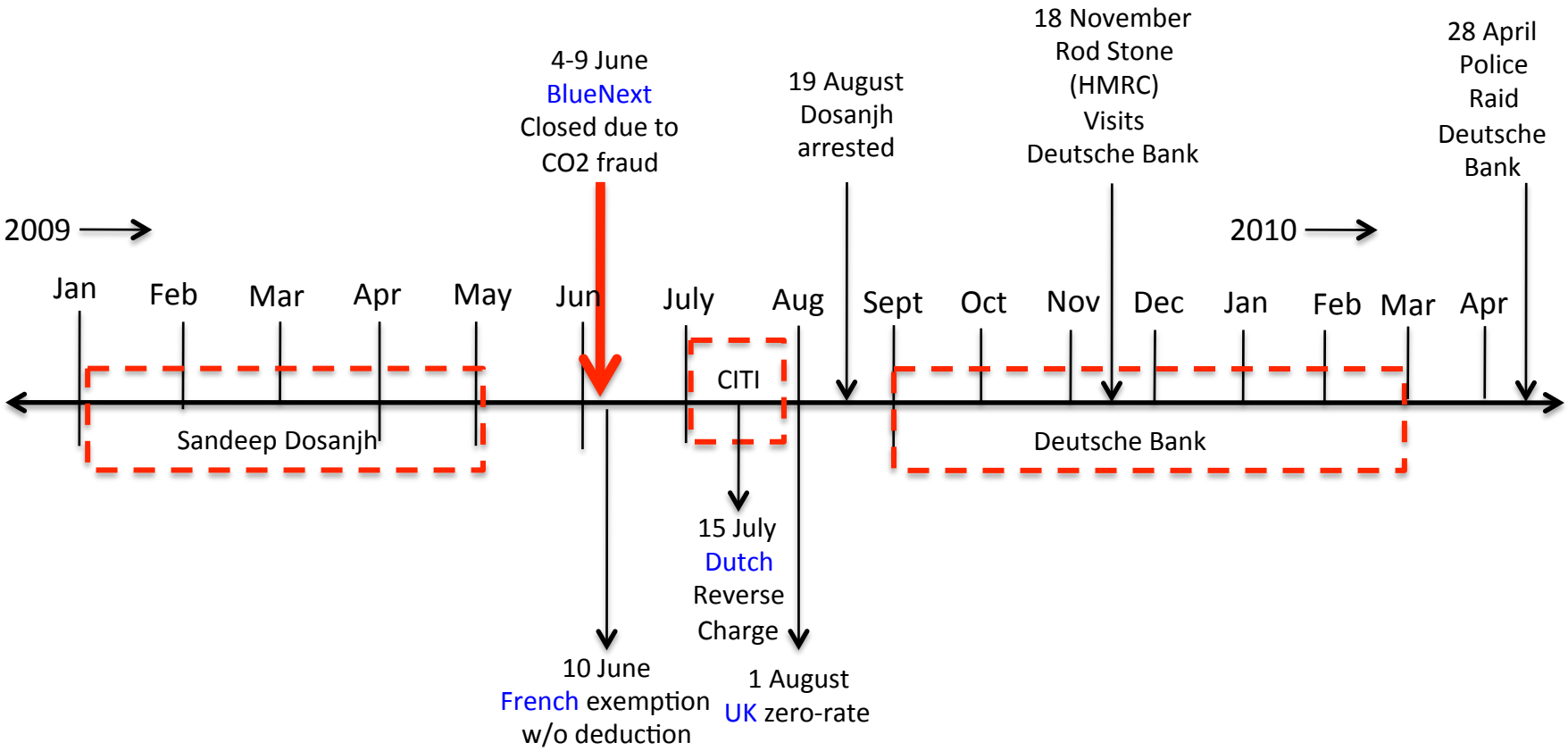
Audits/ Investigations will change

- Consensus forces closer domestic examinations of businesses:
  - Letter box entities
  - Hijacked businesses
  - Financial capacity to accept risk
  - Payments sent off-shore
- Example: Deutsche Bank involvement in CO2 MTIC fraud (2009-2010)
  - Afghan, Pakistani, UK, French, UAE investigations
  - On-going litigation in 2016

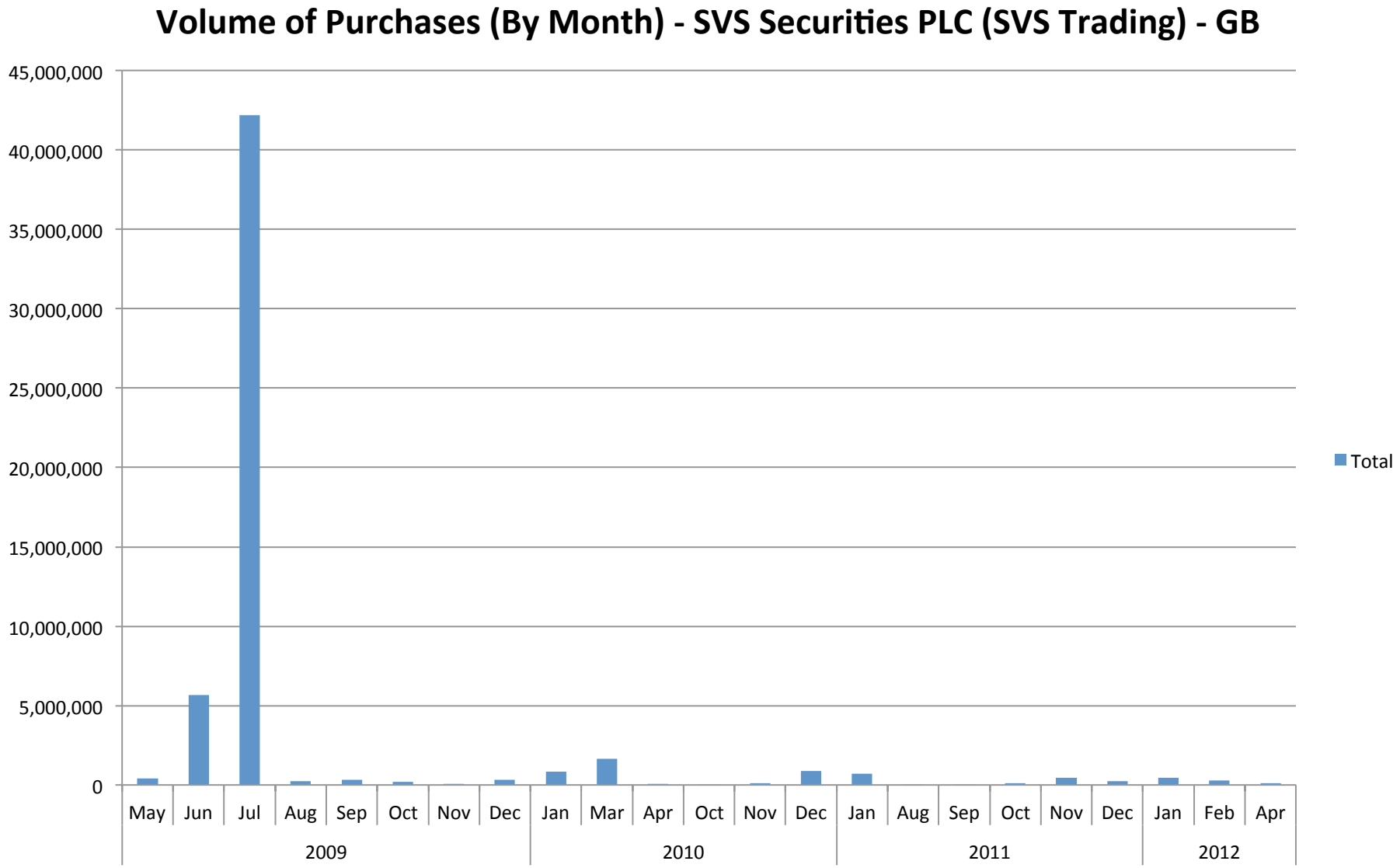
To “get” the examples, you need to know …

- CO2 permit
- EU-ETS [European Union – Emissions Trading System] – this is “cap & trade”
  - Not a tax system – just digital record-keeping of trades in real-time
  - No prices of CO2 permits recorded, no VAT amounts recorded, just volumes of sales (seller & buyer) and precise time of sale (down to the millisecond)
  - And the specific number of the permit

Time-line: CO2 MTIC fraud cases and law changes considered before & after collapse of the BlueNext

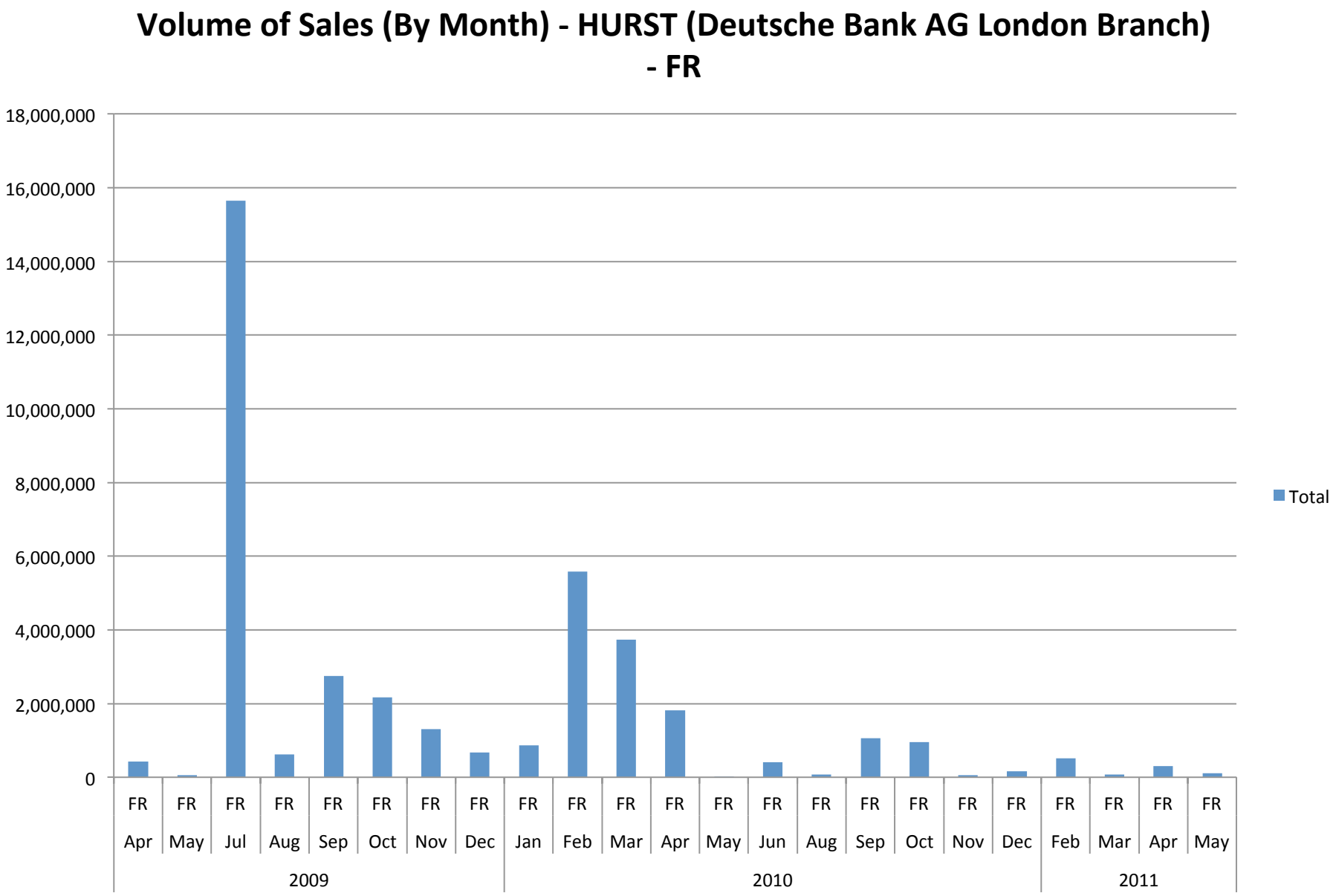


Post-Blue Next collapse (June) & Pre-Zero-rate (August)
UK feeder company selling to UK Deutsche Bank (then export for UK refund)

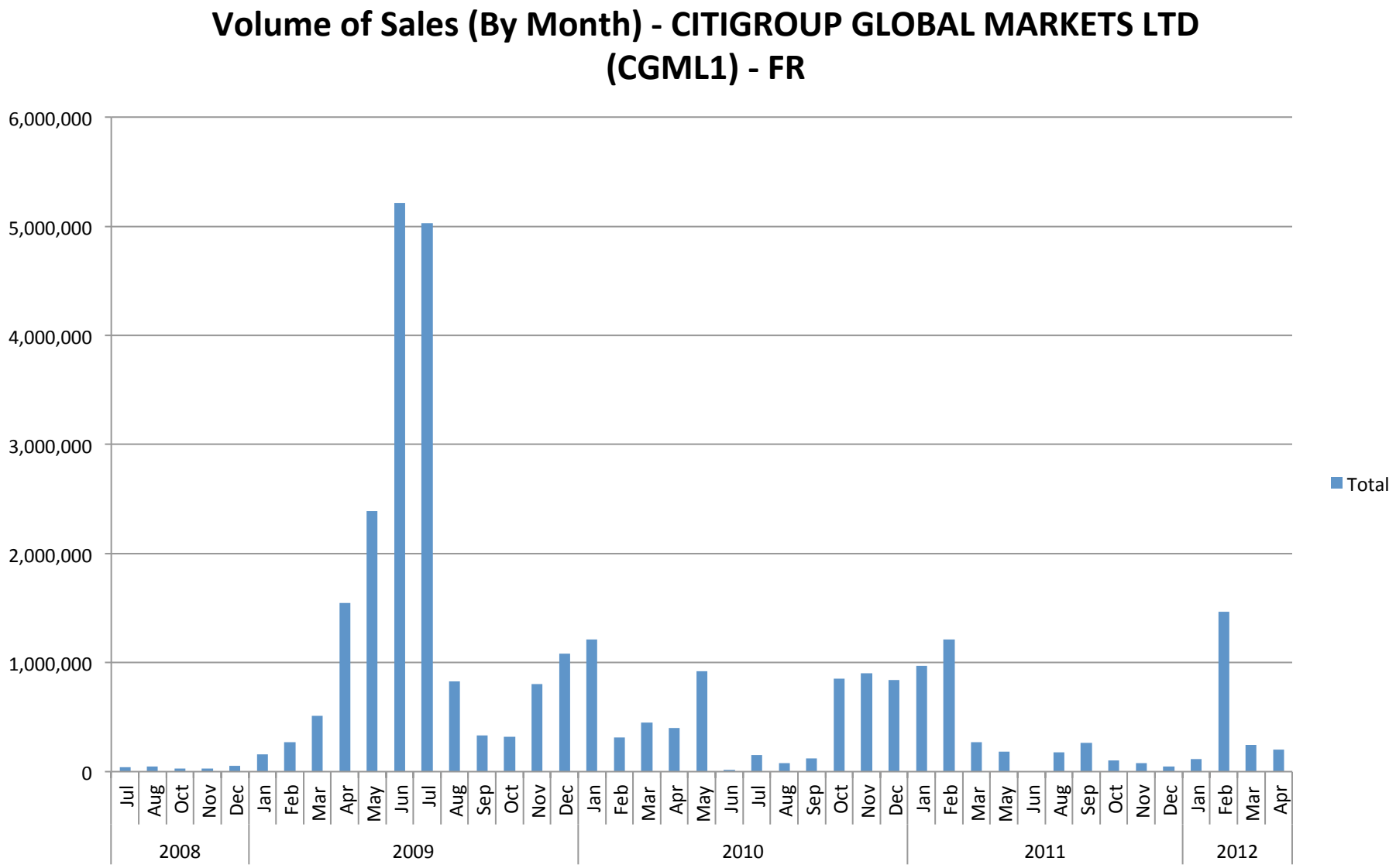


What does Deutsche Bank do with the purchases from SVS ? Sell in France

UK refund

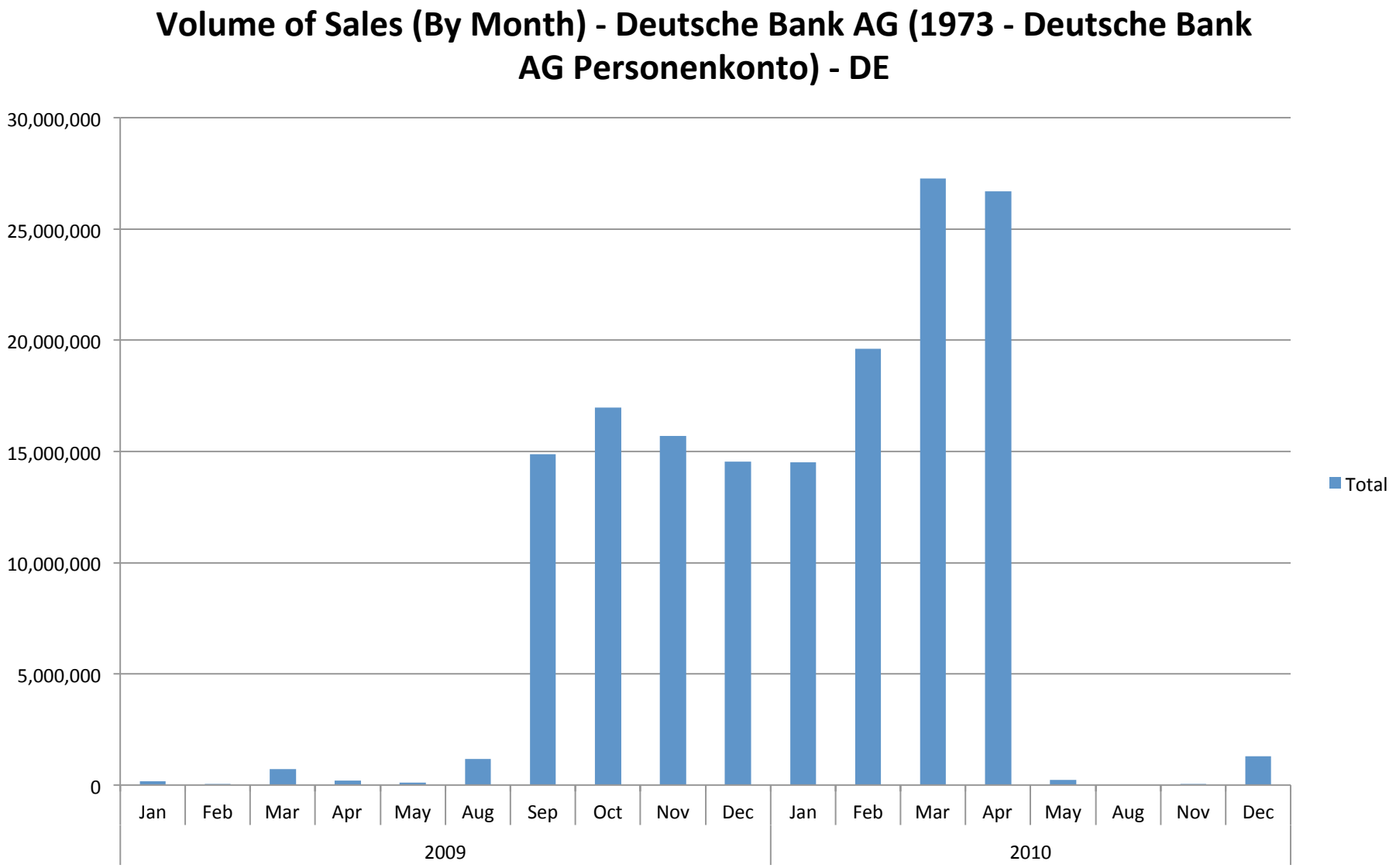


CITIBank (UK) – Does the same thing (Note June & July activity
UK sales to France (from FR account) – **UK refunds**



Reverse Plumbing

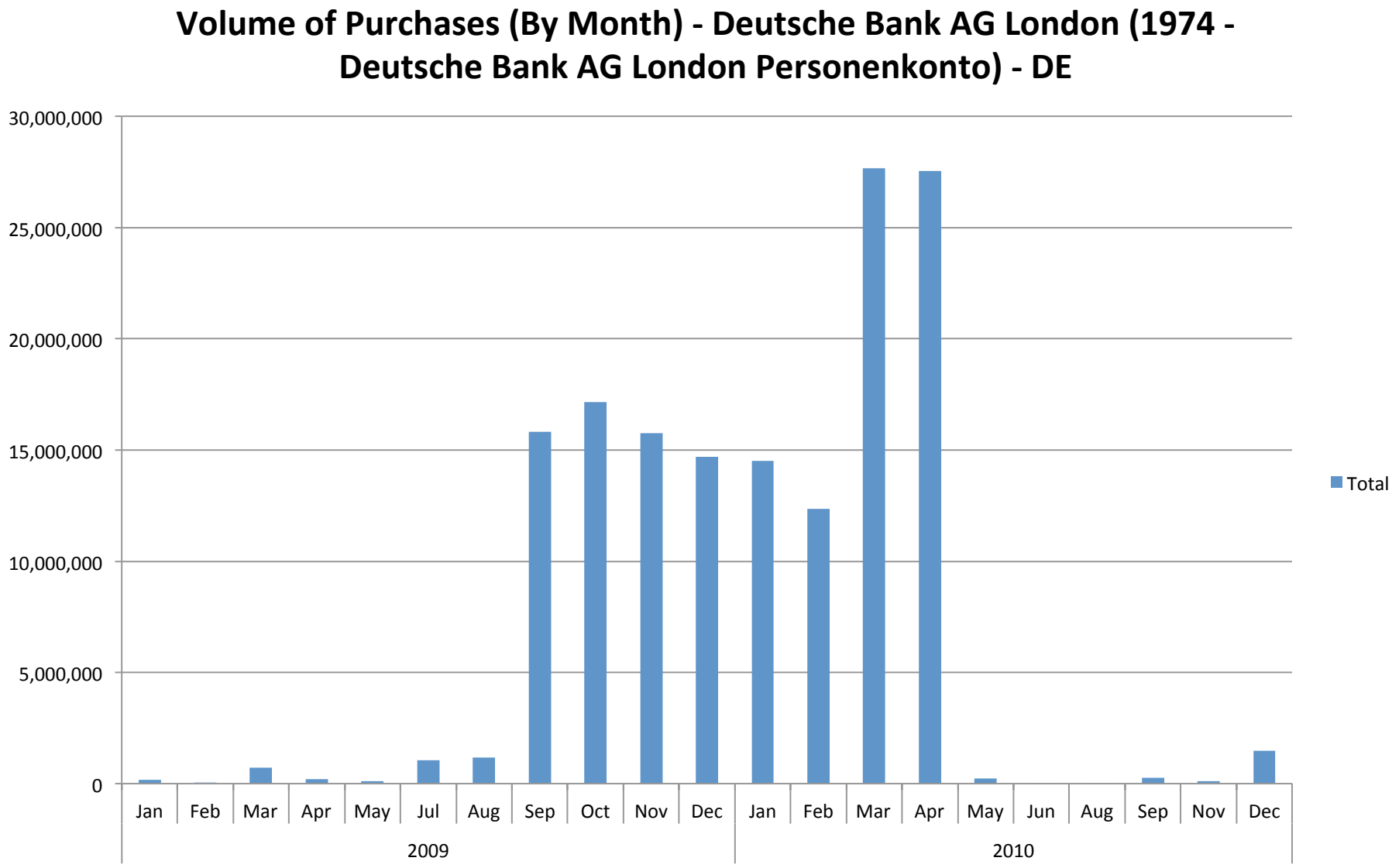
Deutsche Bank German sales to Deutsche Bank UK – **German refunds**



Seen from the other side

Deutsche Bank UK Purchases from Deutsche Bank Germany (internal Deutsche Bank)

UK can see huge German refunds – UK is zero-rated



Who did the German Deutsche Bank purchase CO2 from (after the UK zero-rate) ?

DB-AG 1973		
Lösungen 360 GmbH	31%	52,323,771
Vektor Energie GmbH	14%	24,385,000
Dr. Plathner – New Energy Markets	14%	23,332,000
BECOMAC GmbH	8%	13,440,000
Grant Bank GmbH	7%	11,158,831
Roter Stern GmbH	6%	8,740,420
AEM Alternative Energy Markets GmbH	5%	7,002,000
DB-AG Personenkonto (2)	3%	3,767,686
Advantag Aktiengesellschaft	2%	2,150,000
DB-London Branch	2%	1,170,468
Lösungen 360 GmbH	1%	1,000,000
TOTAL	74%	123,221,191
x €15		1,848,317,865
x 19%		**351,180,394**

DE account
Convicted & sentenced
Convicted & sentenced
Liquidation/ insolvency
Dr. Pilgrim "mystery" came from exchanges infiltrated CO2 markets
Convicted & sentenced

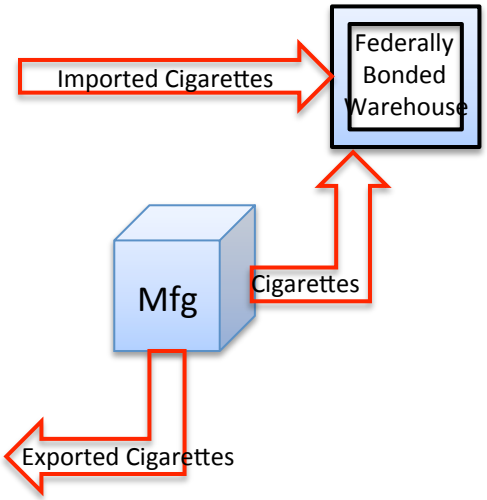
DK account
Convicted & sentenced

Cigarettes

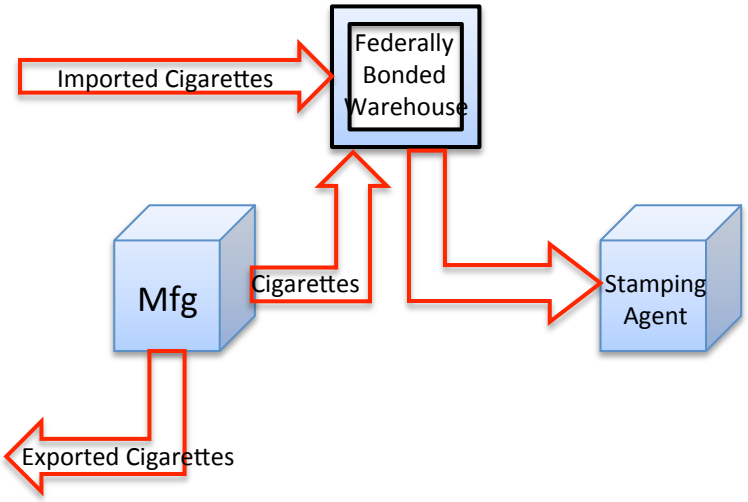
$5 billion/ yr – US States

$50 billion/ yr – global

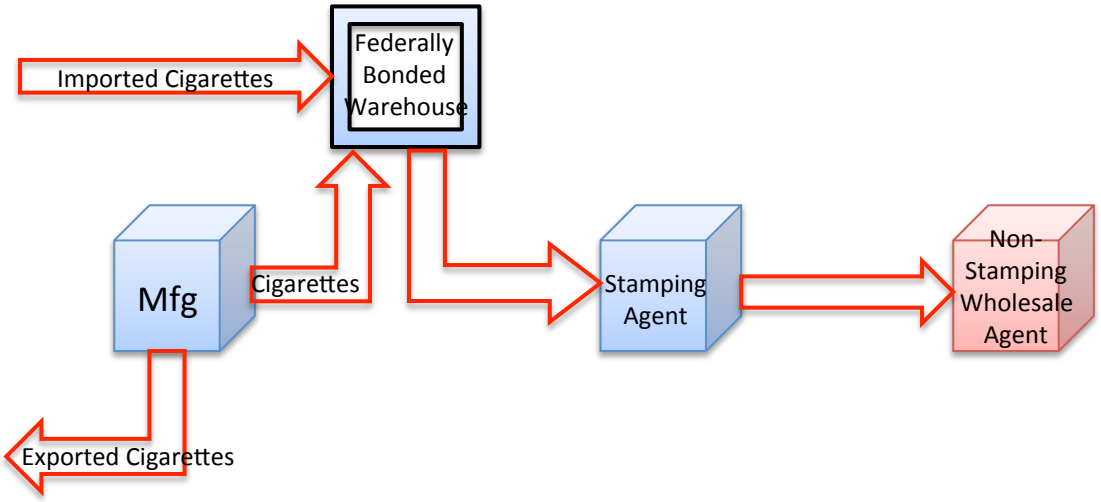
Commercial Chain [1]



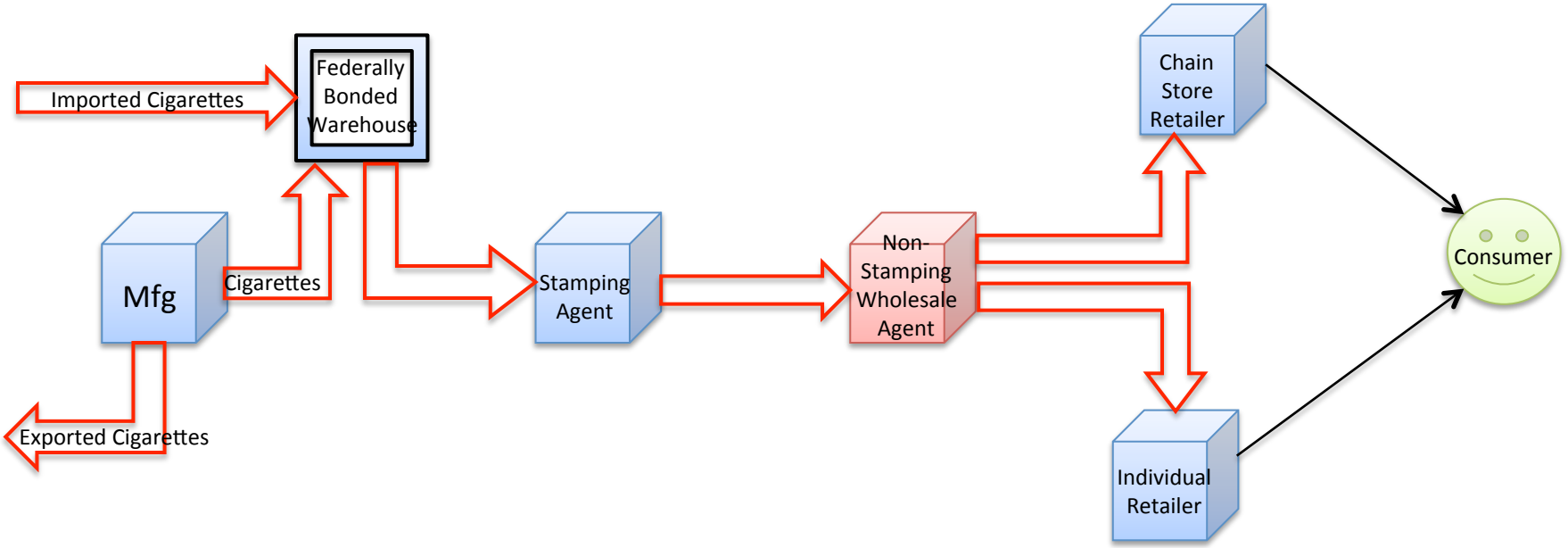
Commercial Chain [2]



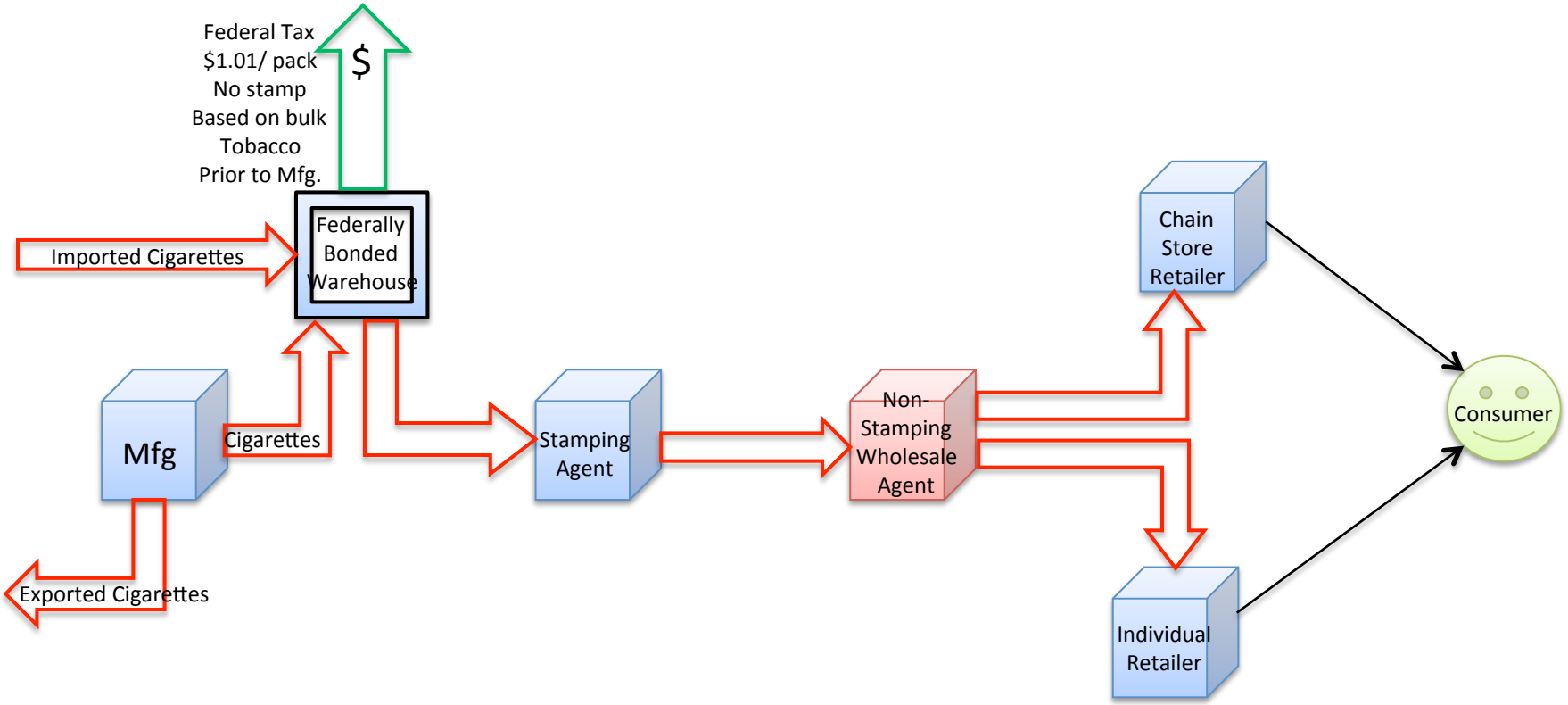
Commercial Chain [3]



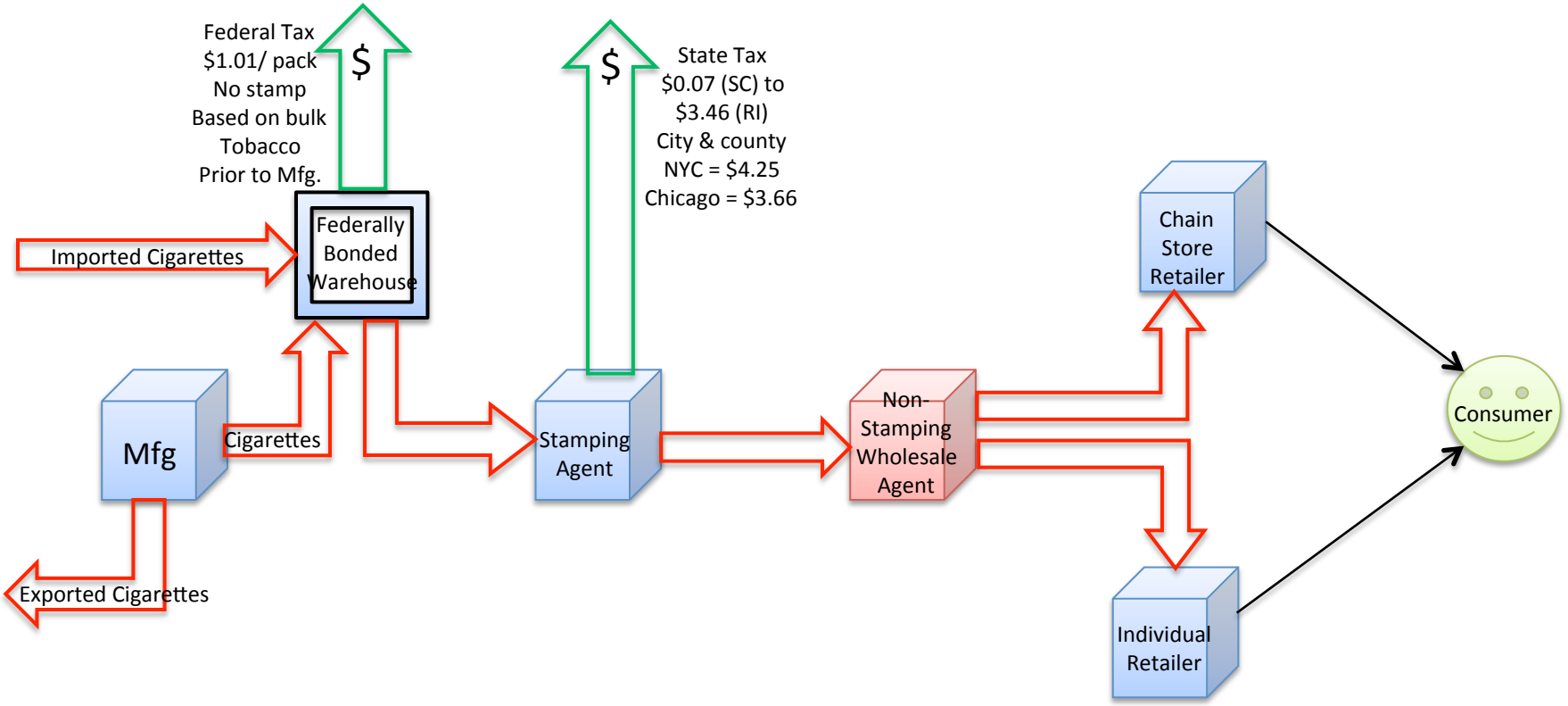
Commercial Chain [4]



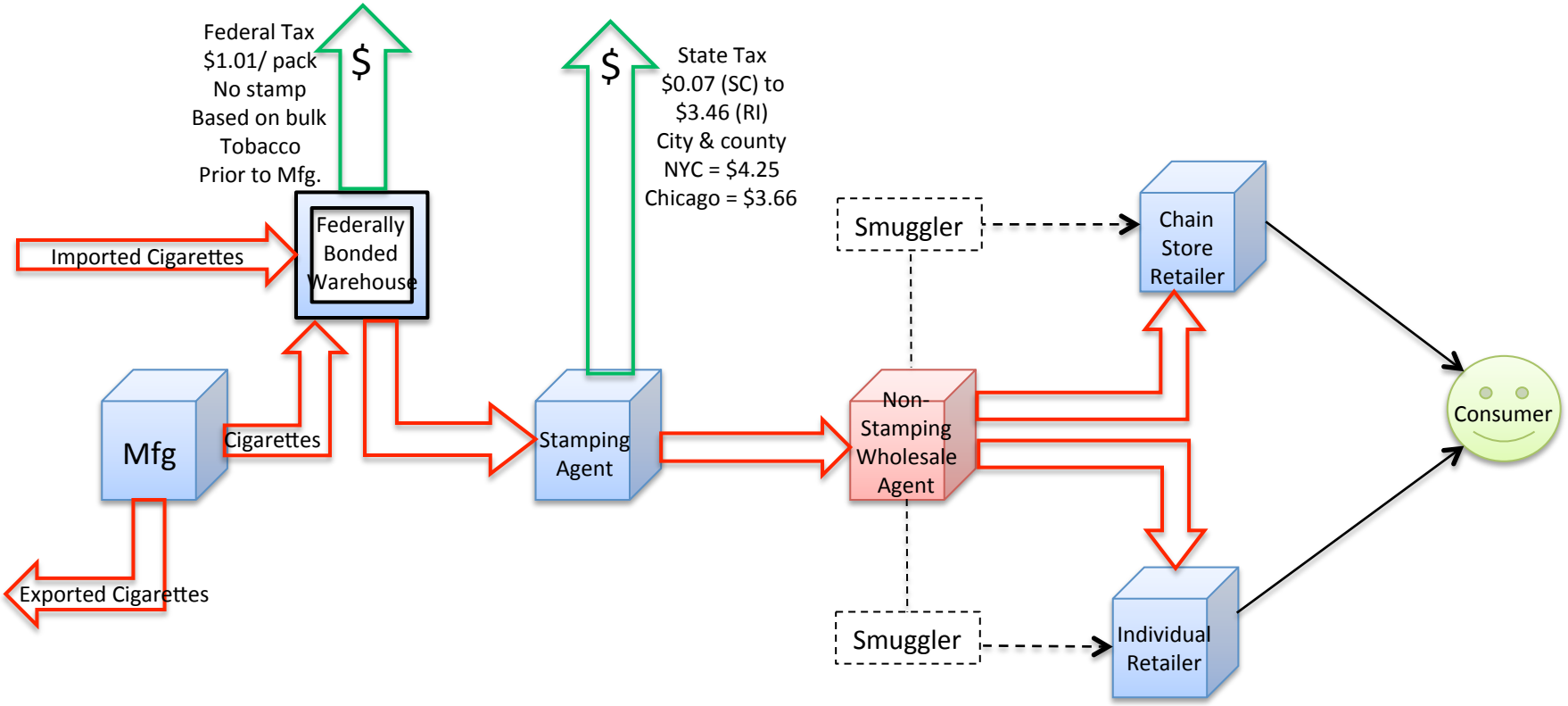
Fed tax


Federal Tax
$1.01/ pack
No stamp
Based on bulk
Tobacco
Prior to Mfg.
$
Federally
Bonded
Warehouse
Imported Cigarettes
Mfg
Cigarettes
Exported Cigarettes
Stamping
Agent
Non-
Stamping
Wholesale
Agent
Chain
Store
Retailer
Individual
Retailer
Consumer

State Tax


Federal Tax
$1.01/ pack
No stamp
Based on bulk
Tobacco
Prior to Mfg.
$
State Tax
$0.07 (SC) to
$3.46 (RI)
City & county
NYC = $4.25
Chicago = $3.66
$
Federally
Bonded
Warehouse
Imported Cigarettes
Mfg
Cigarettes
Exported Cigarettes
Stamping
Agent
Non-
Stamping
Wholesale
Agent
Chain
Store
Retailer
Individual
Retailer
Consumer

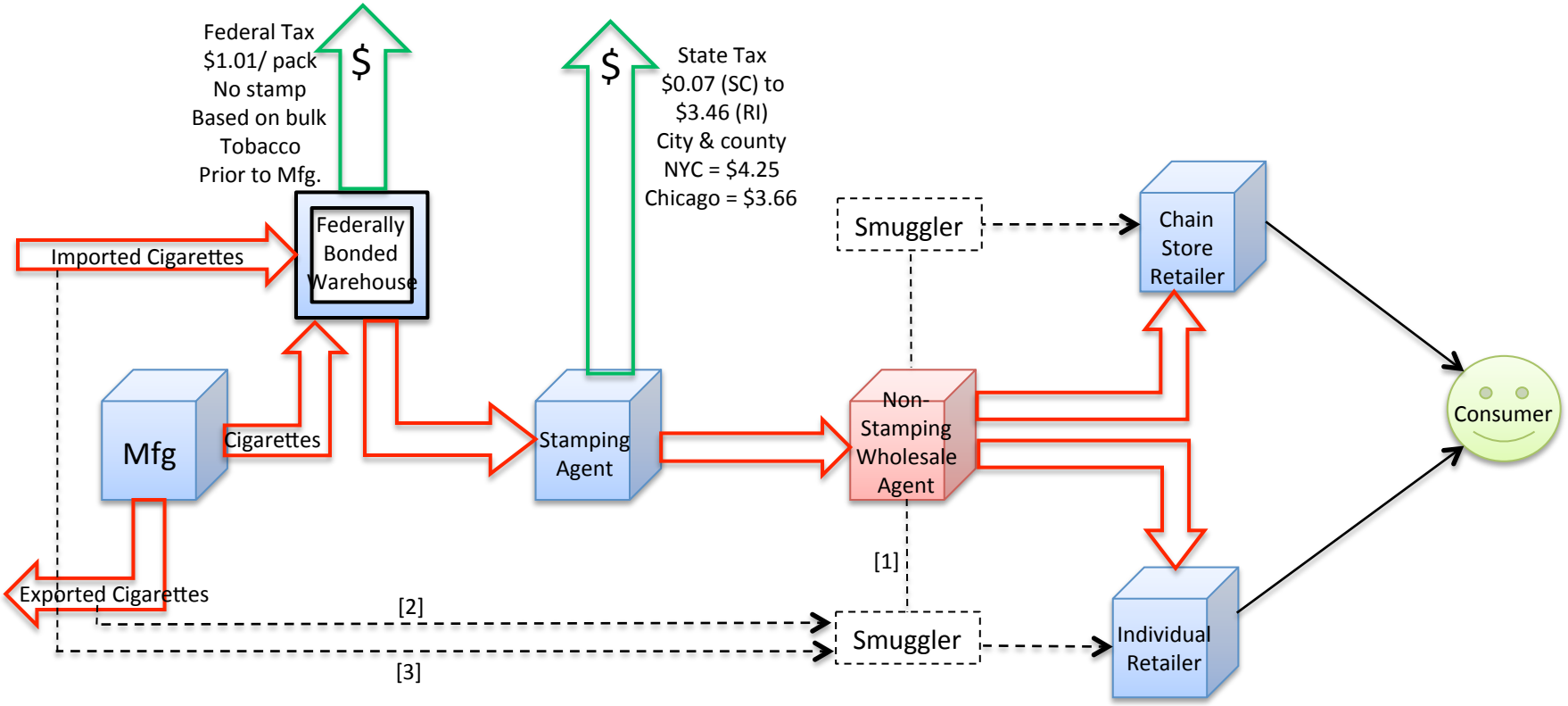
Primary source of Smuggled Cigarettes



Secondary Sources of Smuggled Cigarettes

(2) Acquire Imports before federally bonded warehouses

(3) Acquire "exports" that never leave



Problem

- Enforcement is needed by jurisdictions that will not benefit financially from it:
  - Enforcement resources:
    - US Federal
    - Virginia
    - North Carolina
    - South Carolina
  - Revenue benefits:
    - NYC
    - Chicago
    - Rhode Island

Car load = $23,000 (10 cases)
Van load = $90,000 (50 cases)
Small truck load = $465,000 (200 cases

Primary Legal Tools (federal)

State Statutes Apply Also

- IRC (26 USC Ch. 52)
- Contraband Cigarette Trafficking Act (CCTA) (18 USC Ch. 114, 2341 - 2346)
- Jenkins Act (15 USC 375-378)
- Prevent All Cigarette Trafficking Act (PACT Act) (amends Jenkins Act and CCTA)
- Family Smoking Prevention and Tobacco Control Act

CCTA

- Federal crime to ship, sell transport or possess more that 10,000 cigarettes (500 packs) per month not bearing the tax stamp of the jurisdiction where found
  - 5 years
  - Seizure
  - Predicate crime for RICO

Jenkins Act

- Requires interstate cigarette retailer:
  - Register with state where it sells or advertises
  - File a report with state
    - Quantity
    - Name & Address
  - Federal misdemeanor
    - $1,000
    - 6 months (increased to 3 years under PACT)
- Limited effectiveness – retailers ignore

PACT Act

- Internet-based evasion
  - Requires internet sellers to collect state and local taxes
  - Bans (most) US Post Office delivery of cigarettes
    - State agreements with major private carriers (also) block internet sellers from shipment.
  - Penalties
    - 3 years
    - Civil & monetary fines

Blockchain Solution

- Federal platform
- Mandate transmission of transaction data (at each stage of the commercial chain) to cloud
- Adopt a consensus mechanism:
  a) Permissioned consensus (limited to state & federal enforcement agency employees)
  b) Permissionless consensus (include public)
  c) Hybrid consensus is possible

Step-by-Step

- STEP 1: put secure "trusted bar code" on each pack (inside & out)
  - Regulate under IRC § 5741
  - See: US Patent US 2013/0001291 A1 (Jan. 3, 2013)
- STEP 2: require essential data of all cigarette transactions (B2B and B2C) to be encrypted, and sent to the cloud (free app)
  - License (mandatory registration) of resellers (nationally)
  - Driver's license scan for all B2C transactions
  - Condition tobacco-related business licenses on compliance;
  - Adopt "smart contract" enforcement.
- STEP 3: secure/ validate the commercial chain through a blockchain consensus mechanism (private/public/hybrid)
- STEP 4: require retail to install public "tax paid" verification scanners (free & available on net also)
- STEP 5: allow public access to the blockchain and reward "miners" who find instances of fraud under various False Claim statutes – Find A Fraud Get A Reward campaign.

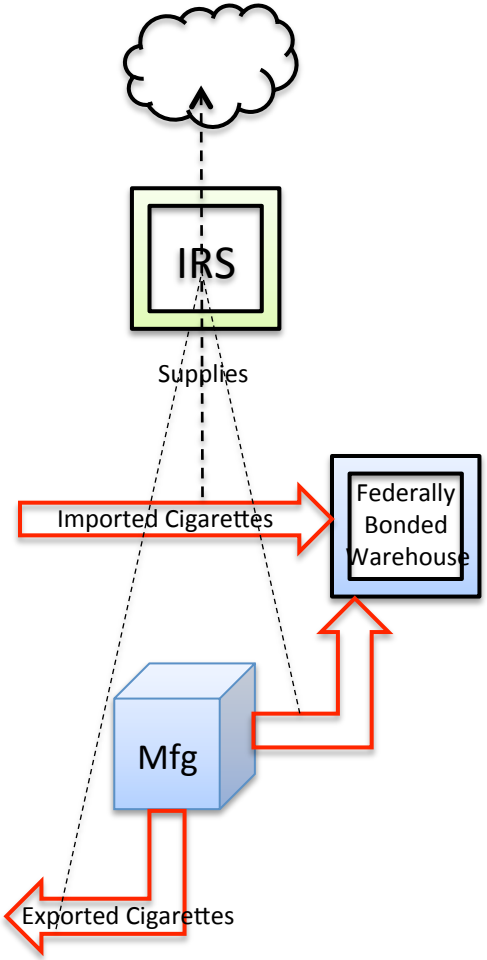
IRC § 5741 - Records to be maintained

- Every manufacturer of tobacco products, processed tobacco, or cigarette papers and tubes, every importer, and every export warehouse proprietor shall keep such records in such manner as the Secretary shall by regulation prescribe. The records required under this section shall be available for inspection by any internal revenue officer during business hours.

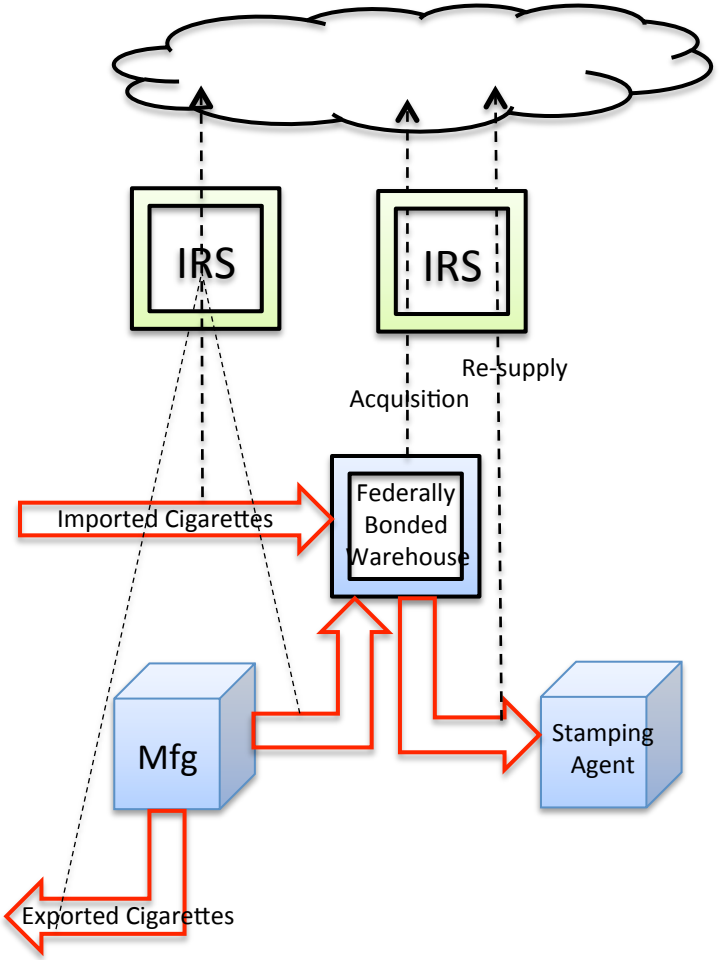
- [Regulate use of a secure trusted bar code under IRC § 5741]

(Aug. 16, 1954, ch. 736, 68A Stat. 715; Pub. L. 85–859, title II, § 202, Sept. 2, 1958, 72 Stat. 1423; Pub. L. 89–44, title V, § 502(b)(9), June 21, 1965, 79 Stat. 151; Pub. L. 94–455, title XXI, § 2128(c), Oct. 4, 1976, 90 Stat. 1921; Pub. L. 111–3, title VII, § 702(a)(3), Feb. 4, 2009, 123 Stat. 108.)

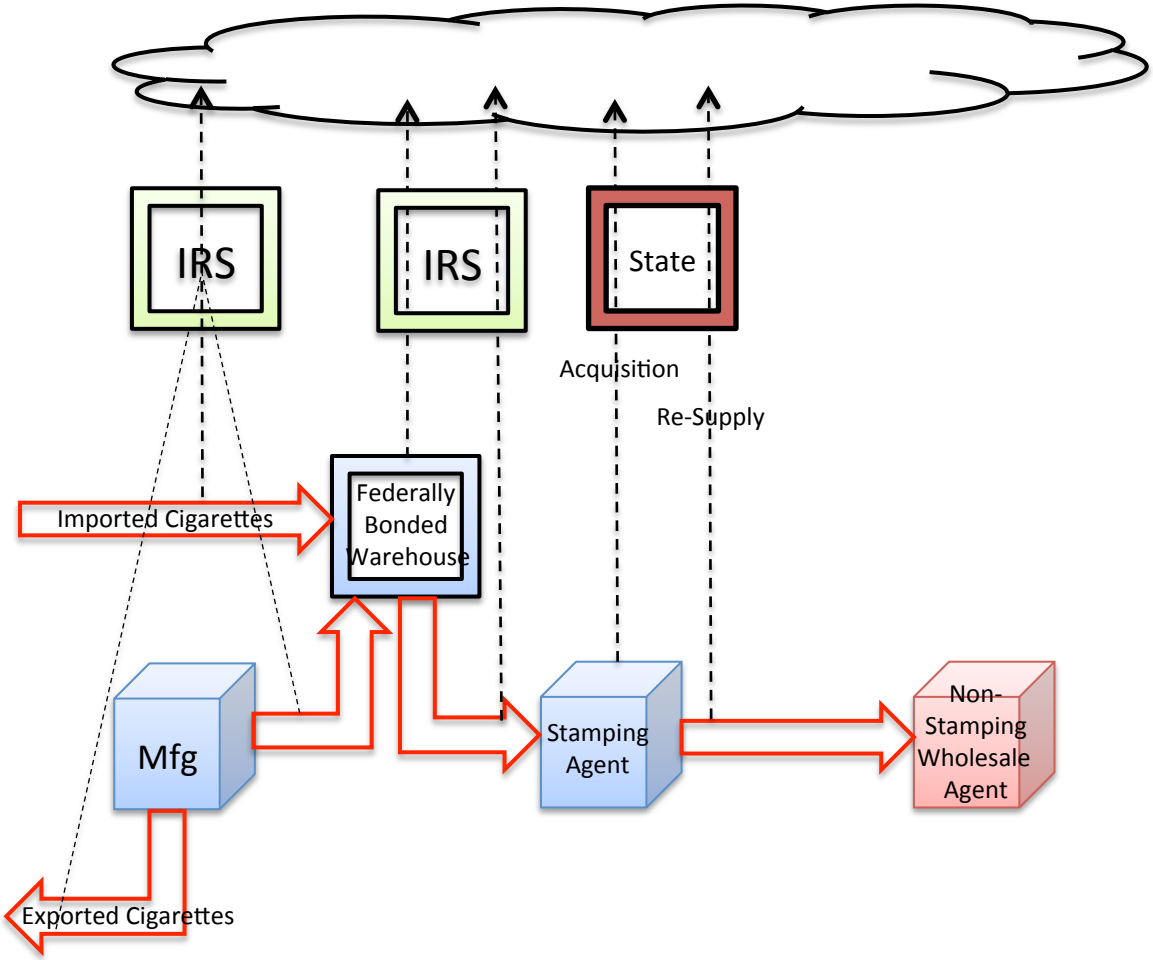
Into the Cloud [1]



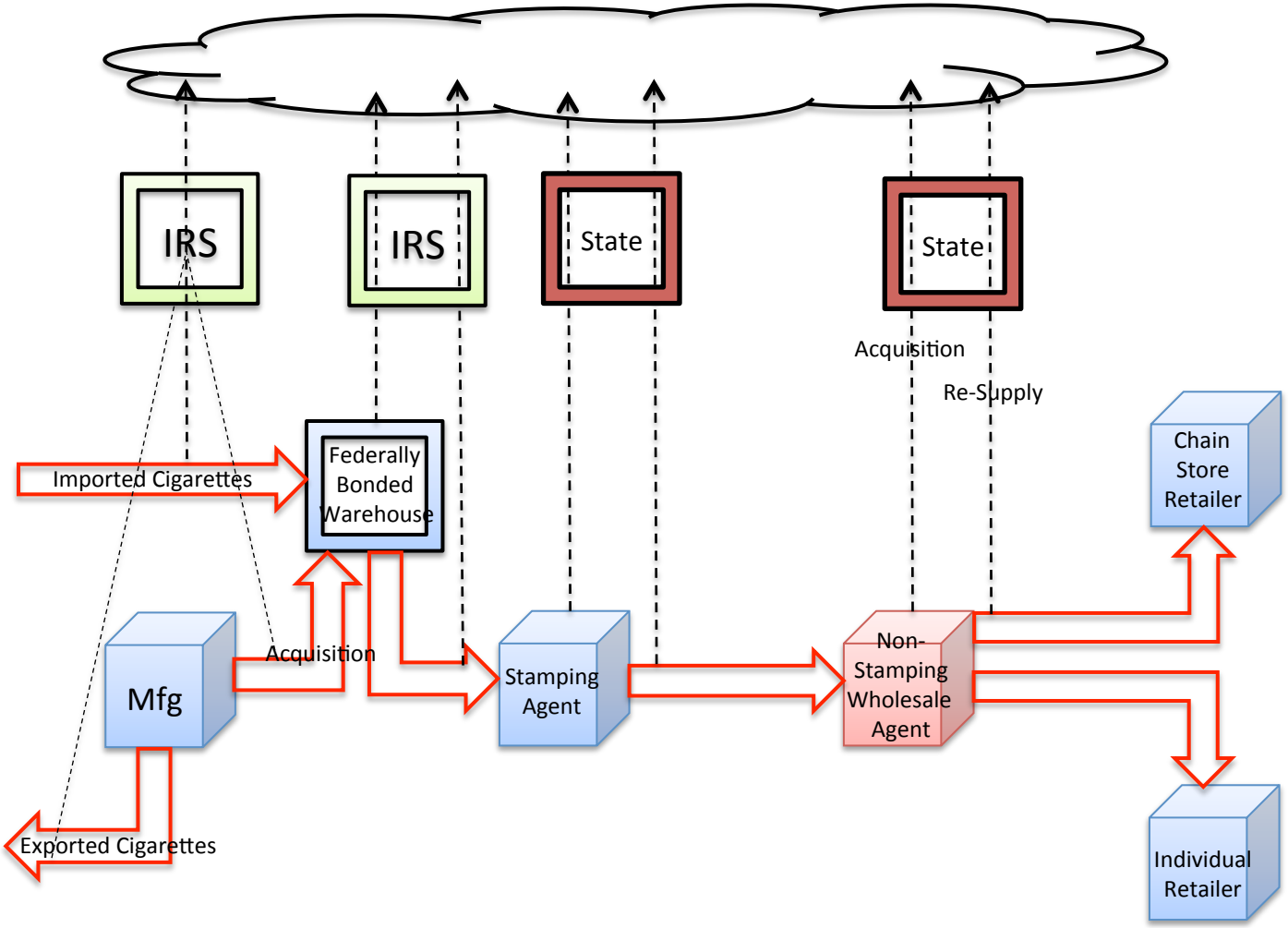
Into the Cloud [2]



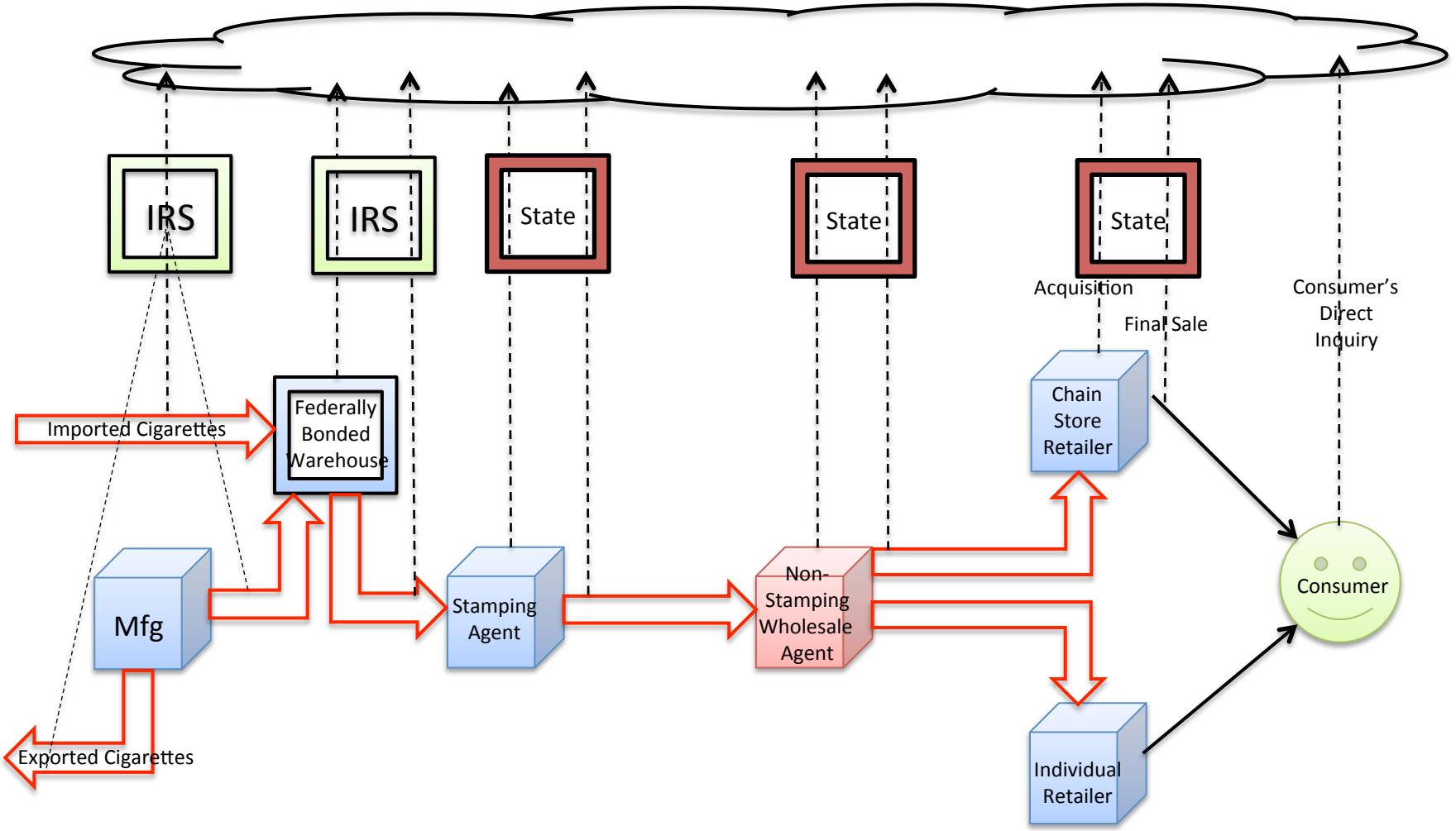
Into the Cloud [3]



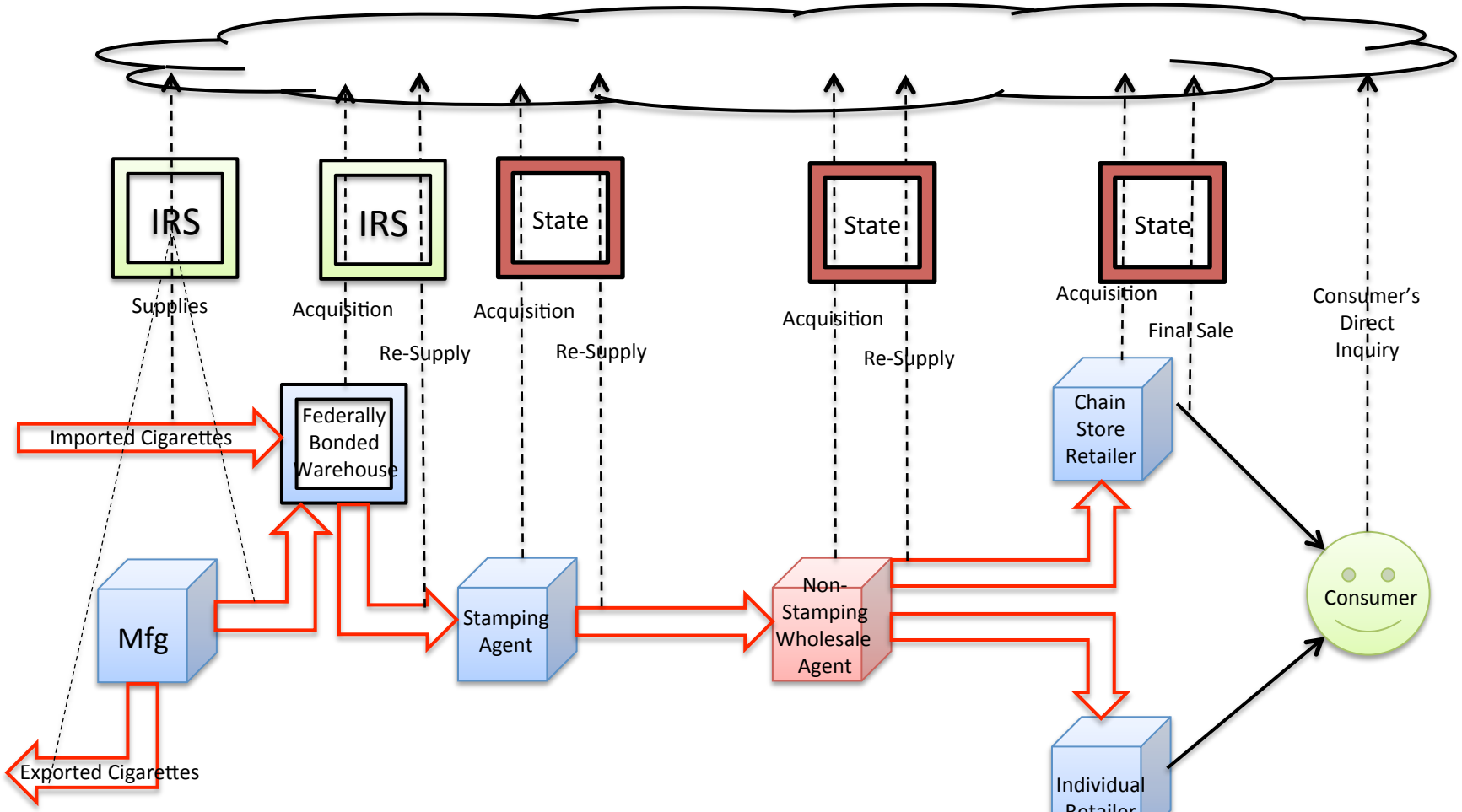
Into the Cloud [4]

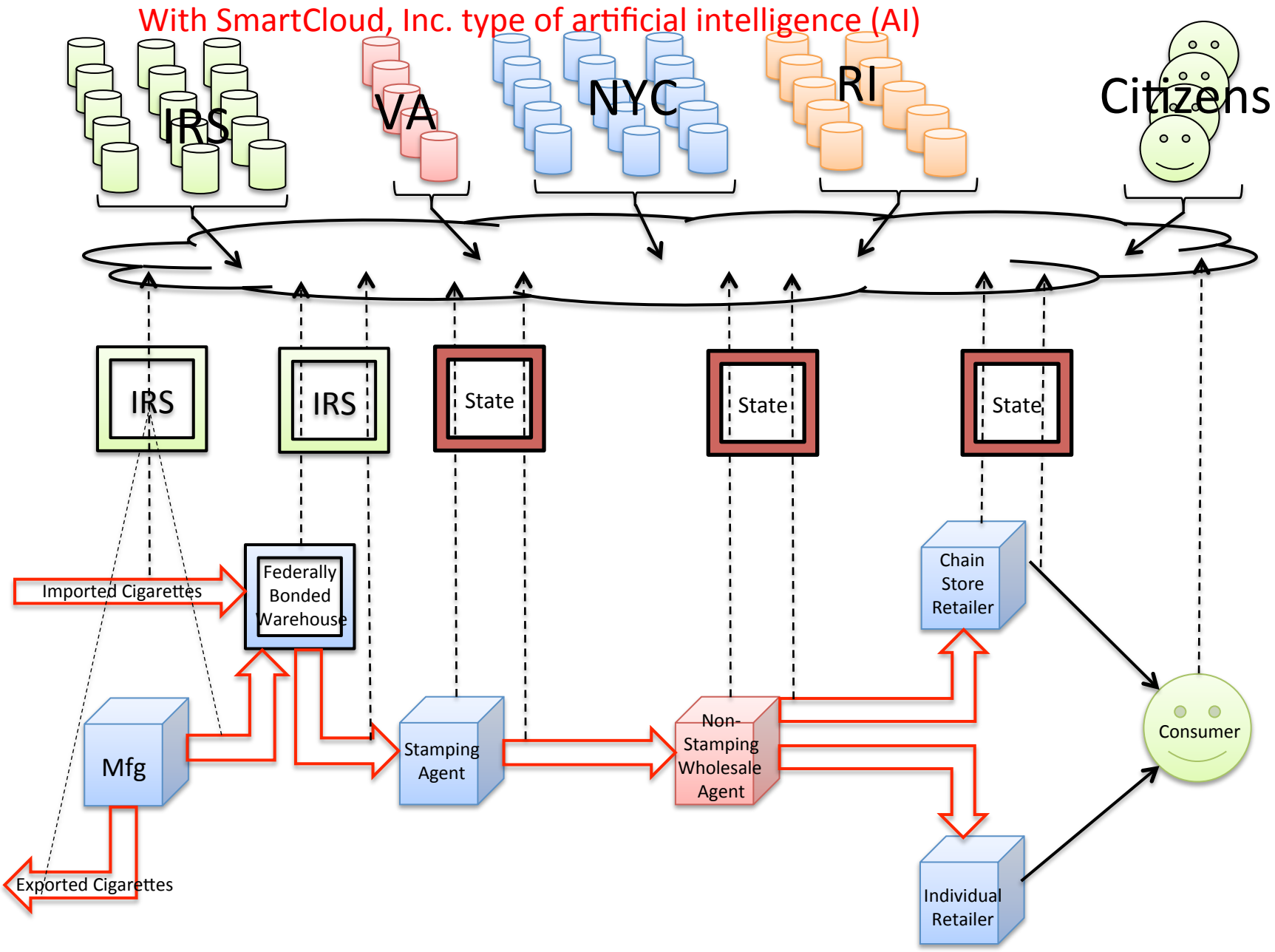


Into the Cloud [5]



Into the Cloud [6]




With SmartCloud, Inc. type of artificial intelligence (AI)
IRS
VA
NYC
RI
Citizens
IRS
IRS
State
State
State
Imported Cigarettes
Federally Bonded Warehouse
Chain Store Retailer
Mfg
Stamping Agent
Non-Stamping Wholesale Agent
Consumer
Exported Cigarettes
Individual Retailer

Final Details

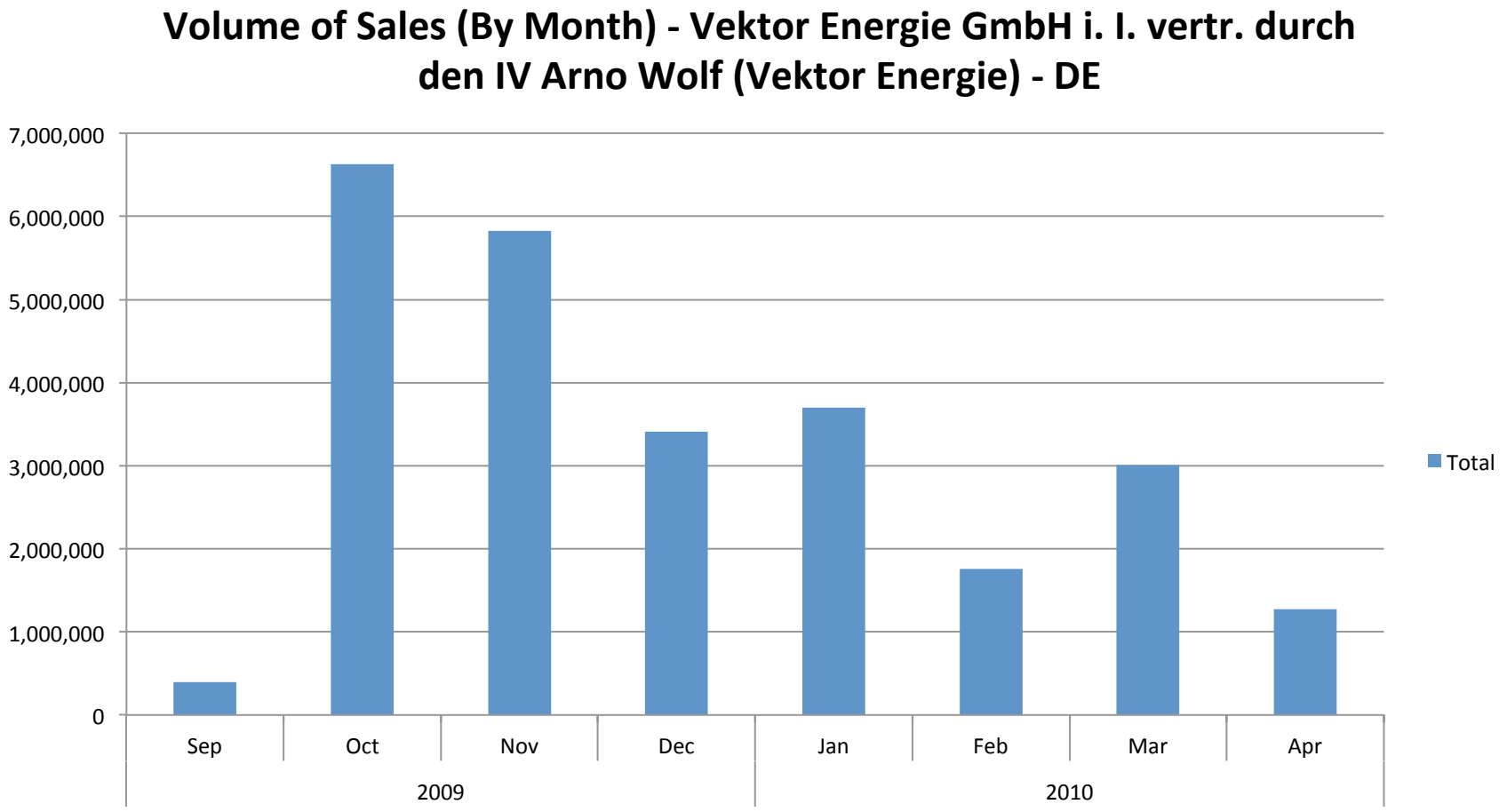
- Where do you get the blockchain platform?
  - Sawtooth Lake … see: HyperLedger Project (its free)
  - http://intelledger.github.io/introduction.html
- How do you securely encrypt data, and get it to the cloud?
  - Try the INTEL chip (for a hardware solution)
    - http://www.intel.com/content/dam/www/public/emea/xe/en/documents/solution-briefs/iot-fiscal-platform-solution-brief.pdf
    - http://www.intel.com/content/www/us/en/retail/solutions/videos/fiscal-compliance-solution-video.html
  - Try a fully digital solution [Data Tech International] a free app for iPhone, or tablet.
- How do you monitor the commercial flows?
  - Adopt the Fed. Energy Reg. Comm. unified data-base & visualization system set up by SmartCloud, Inc.

Faisal Zahoor Ahmad
36 years old & €58 million

Final Example

- Vektor Energie GmbH
  - Founded by 29 y/o UK national on March 31, 2009
  - One-man rented office – only bought & sold CO2
  - Transactions from September 28, 2009 – April 27, 2010
    - UK zero-rate August 1, 2009
    - German raid on Deutsche Bank April 28, 2010
  - Purchased CO2 (mostly from fraudsters) in Germany
  - Sold CO2 93.79% (24,385,000 units) to DB-Frankfurt
  - @€15/unit this is €365,775,000
  - Most days have single (rarely more than 5) transactions
  - Surrendered (voluntarily) in 2016 (currently in jail)

If you knew that CO2 fraud was common, and if SmartCloud Inc. gave you the following report … what would you do in October ?



Thanks

Richard T. Ainsworth

prof482@bu.edu

Richard.Ainsworth@nyu.edu