taxnotes® international

Volume 83, Number 13 ■ September 26, 2016

Blockchain Technology Might Solve VAT Fraud

by Richard T. Ainsworth and Andrew Shact

Reprinted from *Tax Notes Int'l*, September 26, 2016, p. 1165

SPECIAL REPORT

Blockchain Technology Might Solve VAT Fraud

by Richard T. Ainsworth and Andrew B. Shact

Richard T. Ainsworth

Andrew B. Shact

Richard T. Ainsworth is the director of the Boston University graduate tax program and an adjunct professor at the New York University graduate tax program. Andrew B. Shact is vice president of tax and treasury at Mimecast in Boston.

Ainsworth would like to thank his spring 2016 NYU VAT class for engaging him on blockchain during his presentation on missing trader intra-Community fraud and the digital invoice customs exchange solution. Productive discussions continued with Shact.

In this article, the authors discuss how blockchain, a cryptographic software technology, can be used to improve VAT collection and combat fraud.

At the World Economic Forum in Davos, Switzerland, January 20-23, 2016, more than 800 technology executives and observers were asked when they think governments will begin collecting taxes using blockchain, a type of cryptographic software. The average response was 2023, with 73 percent of respondents saying 2025.[1] The survey did not ask respondents to name the tax collected or the jurisdiction that would collect it, so we do not know where they expect blockchain to be used or what they expect it to collect.

This article argues that the EU VAT will be an early adopter, if not the earliest adopter, of blockchain, which will bring substantial efficiency to VAT collection and reduce costs and build trust in intergovernmental relationships. Most importantly, it will immediately end revenue losses of €50 billion to €60 billion per year in missing trader intra-Community (MTIC) fraud.[2]

The European Commission is eager to adopt new technologies in fraud prevention and detection. More effective data sharing and adoption of sophisticated artificial intelligence (AI) programs is critical in that effort. Member states need new ways to share information ''to rapidly and more effectively identify and dismantle fraudulent networks.''[3]

Blockchain will also be essential for the commission's April 2016 VAT action plan and should be a critical part of a legislative proposal expected next year. The plan will introduce a definitive VAT system to address intra-EU cross-border trade based on taxation in

[1] Kimberly Johnson, ''So, What Is Blockchain?'' *The Wall Street Journal*, June 20, 2016, at R6.

[2] The VAT gap is estimated to be between €151 billion and €193 billion, with the MTIC fraud *in goods* portion of this loss to be €50 billion to €60 billion. EY, *Implementing the ''Destination Principle'' to Intra-EU B2B Supplies of Goods — Feasibility and Economic Evaluation Study*, TAXUD/2013/DE/319 (June 30, 2015). Note that the EY study and its estimates are based on goods transactions. Both the VAT gap and MTIC fraud are just as common in services as in goods. The most recent large-scale MTIC frauds are in CO_2 permits and voice over internet protocol. These are service-based frauds. Losses from these frauds far exceed those from goods.

[3] European Commission, ''Action Plan on VAT, Towards a Single EU VAT Area — Time to Decide, COM(2016) 148 final (Apr. 7, 2016), at 6.

the country of destination.[4] This article predicts that the EU will bring in that definitive system on the back of blockchain technology.

Blockchain

Blockchain technology creates a strong, secure, transparent distributive ledger, a revolutionary technique.[5] The software protocol based on cryptography was devised in 2008 and announced simultaneously with bitcoin, its most famous application.[6] Distributive ledgers are not limited to cryptocurrencies and can replace any centralized ledger system that coordinates valuable information.[7] When used, blockchain is highly disruptive to legacy systems. For example, the use of the bitcoin application run on blockchain technology has disrupted commercial banking systems and is expected by the European Central Bank to alter the post-trade market for securities in the EU. In this case, the disruption is in terms of lower reconciliation costs, streamlining the post-trade value chain, and facilitating more efficient use of collateral and regulatory capital. All of these results are economically positive developments, but seen from another perspective, they are highly disruptive to current processes.

Blockchain technology is trustless in the sense that it does not require third-party verification. It does not need a trusted third party (like a bank) to negotiate (exchange) value and instead uses powerful consensus mechanisms with cryptoeconomic incentives to verify the authenticity of transactions in the database.[8] The consensus mechanism makes the database safe (highly trustworthy) even in the presence of powerful or hostile third parties trying to manipulate the registry. For that reason, blockchain has been called ''the trust machine.''[9] The trust element is important to the adoption of blockchain in tax compliance areas.

Only recently have decentralized, distributive ledgers been possible as a result of advances in technology, computing capacity, and connectivity. Replacing expensive centralized ledgers with decentralized distributive ledgers captures huge cost savings and efficiencies.[10] Decentralized distributive ledgers ride three exponentially declining cost curves:

- Moore's Law: the cost of processing digital information is halved every 18 months (speed);[11]
- Kryder's Law: the cost of storing digital information is halved every 12 months (memory);[12] and
- Nielson's Law: the cost of shipping digital information is halved every 24 months (bandwidth).[13]

Bitcoin Blockchain

A bitcoin is a digital asset that is acquired in exchange for other currencies, goods, or services. The coins themselves are created as a reward for payment processing work in which users volunteer computer capacity to verify and record other individuals' transactions, an activity called mining.

Bitcoin is a peer-to-peer payment system using open-source software. Transactions take place between users directly with no intermediary, such as a bank or other trusted third party. They are verified by network nodes and recorded in a public distributed ledger where the bitcoin itself is the unit of account — the blockchain. There is no central depository or administrator.

Bitcoin was the world's first decentralized digital currency. The novelty of bitcoin's blockchain is that it is a public ledger maintained by a network of communicating nodes running the bitcoin software. Network nodes receive a transaction that if validated, is added to their copy of the ledger. That copy is then broadcast to the other nodes. Approximately six times per hour a new group of accepted transactions, or a block, is created.

Bitcoin's public decentralized ledger is accessible by every Internet user. Anyone can participate in the verification process and determine which blocks can be added to the chain.[14] The consensus mechanism is

[4] European Commission release on a VAT action plan, IP/16/1022 (Apr. 7, 2016).

[5] Ledgers have long been digitized, but it was only with blockchain that they have been decentralized.

[6] Satoshi Nakamoto, ''Bitcoin: A Peer-to-Peer Electronic Cash System'' (2008).

[7] Aaron Wright and Primavera de Filippi, ''Decentralized Blockchain Technology and the Rise of Lex Cryptographia'' (Mar. 12, 2015), at 4-8.

[8] Tim Swanson, ''Cryptoeconomics for Beginners and Experts Alike,'' *Great Wall of Numbers* (Jan. 30, 2015), citing Vlad Zamfir of the Ethereum project at the Cryptocurrency Research Group conference (brainstorming session) on Cryptoeconomics. Cryptoeconomics is:

> A formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.

[9] ''The Promise of Blockchain: The Trust Machine,'' *The Economist*, Oct. 31, 2015.

[10] Sinclair Davidson, de Filippi, and Jason Potts, ''Economics of Blockchain'' (2016).

[11] Gordon E. Moore, ''Cramming More Components onto Integrated Circuits,'' 86(1) *Electronics* 114 (Apr. 19, 1965). Moore is the founder of Intel and Fairchild Semiconductor.

[12] Mark Kryder, ''Kryder's Law,'' *Scientific American* (Aug. 2005). Kryder was the senior vice president of research and the chief technology officer at Seagate Corp.

[13] Jakob Nielson, ''Nielson's Law of Internet Bandwidth,'' *Nielson Normal Group* (Apr. 5, 1998). Nielson was an engineer at Sun Microsystems.

[14] Vitalik Buterin, ''On Public and Private Blockchain,'' *Ethereum Blog* (Aug. 7, 2015).

proof of work, which means that the nodes in the network run complicated algorithms to verify each transaction.

Public ledgers are often called unrestricted or unpermissioned ledgers, and private ledgers are often referred to as restricted or permissioned.[15] That is meant to bring into sharp relief white or black listed users, identified through know-your-bank or know-your-customer procedures common in traditional finance. It is clear that private, restricted, or permissioned distributed ledgers work best in a governmental context.[16]

Miners keep the blockchain consistent, complete, and unaltered by repeatedly verifying and collecting new transactions into a block. Each block contains a cryptographic hash of the previous block. Consensus binds the new block to the chain through proof of work. However, there is a moving measure of computational difficulty in reaching proof of work sufficient to secure a new block to the chain.[17]

The expense of time, computational resources, and electricity is problematic for bitcoin's public distributed decentralized ledger and has encouraged developers to search for alternate validation systems. Proof of stake and proof of identity are two alternate consensus processes identified that are well suited for private distributed ledgers.

Older Systems

The VAT information exchange system (VIES) is a database solution to cross-border VAT fraud. It uses old technology and multiple centralized data centers, and a semiautomatic — and frequently manual — data exchange process is involved.

Recently, VIES's largest concern has been MTIC fraud, which annually costs the EU €50 billion in goods-based frauds, and possibly another €50 billion in services-based frauds,[18] which can be extra-Community (MTEC).[19]

The digital invoice customs exchange (DICE) was the outgrowth of an effort to improve the fraud prevention functionality of VIES by developing a more automated and immediate exchange of invoice-level data. DICE involves placing digital signatures on invoices and then feeding encrypted invoice data back into relational databases that match transactions and perform risk assessments across the single market.

Under DICE, transaction data are shared automatically and in advance of performance among the jurisdictions and taxpayers that are parties to a specific transaction. It provides a mechanism for local enforcement against local losses. However, DICE requires that the EU adopt a third invoicing directive.

Brazil's digital invoicing regime demonstrates that a DICE approach to digital control over invoice data works to solve cross-border fraud. Compliance is no more burdensome than swiping a credit card and waiting for approval.

VIES can never provide real-time enforcement. An example of MTIC fraud helps to work through the operation of VIES and DICE. From here we can see how blockchain moves the analysis forward.

Assume Company A in the Netherlands agrees to sell a specific quantity of high-value goods to Company B in France. The price is set, as are the time and method of delivery. In this intra-Community supply, A will zero rate the sale. It will file a return in the Netherlands seeking the return of all VAT paid there — that is, it will seek recovery of the input VAT it paid on purchases related to the sales output. B is expected to perform a reverse charge in France — that is, it will self-assess the French VAT on the goods it purchased and record the transaction on its French return.[20]

MTIC fraud would arise if B does not perform the reverse charge, does not file an accurate French VAT return, does not remit the French VAT due, but still sells the goods to Company C in France with VAT collected on the new selling price.

By not remitting the French VAT, B becomes a missing trader. The fraud is equal to the VAT charged on the onward sale. The French revenue authority must find B quickly, because its owners are likely to leave the country.

The VIES system hopes to detect that fraud by sharing data among tax jurisdictions. Along with A's VAT return, a recapitulative statement is filed with the Dutch tax authority listing the cross-border entities A has sold to and an aggregate amount of sales per entity. The French tax administration can request that data when it audits B.

The timing of that data exchange is protracted. A's VAT return and recapitulative statement may be filed

[15] Swanson appears to have first use the term "permissioned." *See supra* note 8.

[16] Marcella Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" (Dec. 2015), at 16-24.

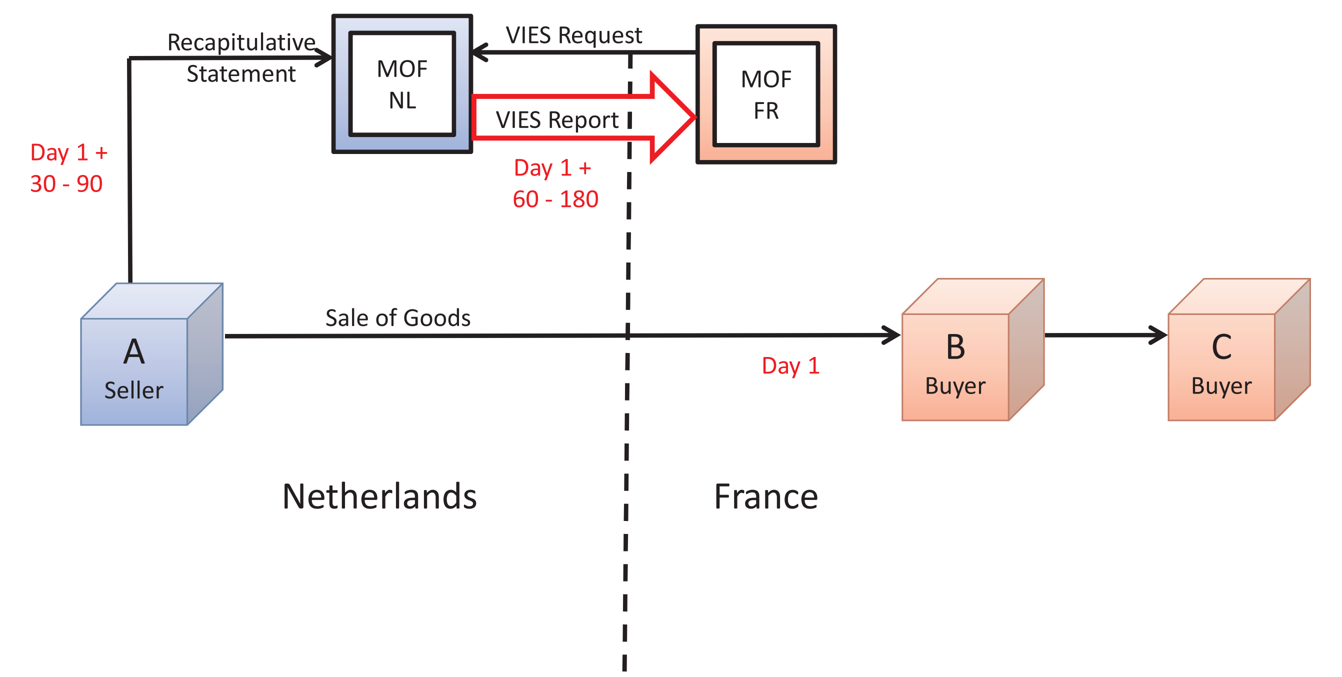
[17] Blockchain Info, "Difficulty History."

[18] Europol, *SOCTA (Serious and Organized Crime Threat Assessment) 2013 — Public Version*, 27 (Mar. 2013) (estimating MTIC fraud losses at €100 billion annually).

[19] Ainsworth, "VAT Fraud: The Tradable Services Problem," *Tax Notes Int'l*, Jan. 17, 2011, p. 217.

[20] Council Directive 2006/112/EC requires the member state making the supply to exempt the transaction with a full right of deduction — sometimes called "zero rating." The member state of acquisition must impose a tax based on the same factors used to determine the taxable amount for the supply of the same goods within that member state. The obligation to pay the tax on the buyer. Thus, a reverse charge is the result. The buyer (rather than the supplier) is obligated to remit the tax. The goods are received tax free.

Figure 1. Basic VIES Operation



one, three, or 12 months after the fraud transaction has occurred, depending on its Dutch filing status. The Dutch authorities must respond to the French request for the data within three months, although an expedited response of one month is possible if the Netherlands already has the information.[21] Figure 1 illustrates that.

The most obvious difficulties with VIES are that it is request based; provides aggregate data, not invoice-level granular data; and the data exchange is delayed at least two to six months after a suspect transaction has occurred. MTIC fraud can be completed much faster than the VIES system can issue a report on it. For example, it took Sandeep Singh Dosanjh only 69 days to complete a €41.5 million MTIC fraud in CO_2 permits.[22] VIES was totally inadequate to identify, much less stop, Dosanjh.

DICE

Previous DICE proposals presumed the tax authorities worked with a centralized database.[23] There were two permutations in those proposals depending on whether the database contained transactional data only from a single tax jurisdiction, as in Rwanda and Ceará, or whether the single database collected tax data from multiple jurisdictions in a community, as in Brazil.

Problems arise when several tax jurisdictions are bound together in a community but each jurisdiction insists on keeping separate central databases of its own tax data. The problem of sharing data among related centralized databases is the main concern that DICE was designed to solve.

How do you efficiently share tax data among the jurisdictions in an economic union when each holds its own data centrally? Security systems are operating at a high level to protect the data, and procedures to grant external access to that data are cumbersome and time consuming. Early DICE articles demonstrated how that process could be streamlined with encryption and sharing of public access keys. However, DICE objectives can be better accomplished through decentralized databases or distributed ledgers.

EU, Rwanda, and Ceará

When DICE was first proposed, it addressed VIES/MTIC fraud problems in the EU.[24] The basic design incorporated elements of Brazil's successful digital invoicing regime into a proposal for a third invoicing

[21] Council Regulation (EU) No. 904/2010 of Oct. 7, 2010, on administrative cooperation and combating fraud in the field of value added taxation, 2010 OJ L-268 1, at article 10.

[22] Ainsworth, ''VAT Fraud Mutation, Part 1: ''Push'' Missing Trader Fraud and Dosanjh,'' *Tax Notes Int'l*, Feb. 8, 2016, p. 535.

[23] Ainsworth and Todorov, ''Stopping VAT Fraud with DICE — Digital Invoice Customs Exchange,'' *Tax Notes Int'l*, Nov. 18, 2013, p. 637.

[24] Ainsworth, ''Stopping EU VAT Fraud With a Third Invoicing Directive,'' *Tax Notes Int'l*, Aug. 5, 2013, p. 545.

directive.[25] It was clear in that proposal that DICE could be used to solve both fraud occurring in a single state and fraud occurring between states in a community, even if the relevant tax data was stored in multiple, centralized databases.

DICE has been successfully implemented in Rwanda;[26] revenue increased 16 percent in the first six months after adoption.[27] There is a potential community application for DICE in Africa. Several other members of the East African Community (EAC) are considering DICE, and a separate proposal has been drafted for the EAC.[28]

It is still unclear how a single EAC database will be set up, but recent events suggest that Tanzania is open to adopting a single centralized data center with Rwanda.[29] The EAC data structure could adopt a multijurisdictional DICE solution similar to what would work in the EU, with each member state keeping its own data center with data shared through encryption and exchange of access keys. It could also be a single centralized system similar to what works in Brazil, with a single data center collecting and coordinating data exchanges among all members.[30]

Another fully developed, single-state adoption of DICE is operational in the Brazilian state of Ceará. It includes a state-of-the-art AI program set up by SmartCloud Inc. that scans all data streams for a real-time risk assessment.[31] SmartCloud provides immediate risk analysis reports, continuously reviews data for fraud patterns, and responds to specific system queries by trained auditors.[32]

DICE in Rwanda and Ceará operate on centralized ledgers, which have three well-recognized, general problems: A centralized ledger is a single point of failure for the whole system, is prone to corruption because it consolidates power, and is inherently insecure. It consumes huge amounts of resources to protect its data.[33]

A fourth problem arises in a VAT context: Centralized ledgers are inherently inadequate as a comprehensive VAT compliance mechanism. A single, jurisdictionally bound database can never capture all relevant transactional data. Centralized ledgers by definition store data only from taxpayers in their jurisdiction. Exceptional measures must be in place whenever confidential data is imported from outside the jurisdiction.

All those problems are resolved when moving to distributed ledgers, such as blockchain.

The original DICE proposal sought to resolve the fourth problem for transactions occurring entirely in the EU. It assumed that the EU would not accept a Community-wide central database. It also assumed that each EU member state would insist on controlling and sharing data held in its own centralized database according to its own rules and procedures. As a result, the proposal assumes there would be 28 independent, centralized databases.

Figure 2 summarizes the data flows between hypothetical Seller A in the U.K. and hypothetical Buyer B in France. XML files are sent to separate U.K. and French data centers, and access keys are exchanged among all authorized parties. Each member state has immediate access to relevant taxpayer data in another member state. Access would be limited to taxpayers and transactions that engaged in cross-border transactions with domestic taxpayers. The proposal is a pure data exchange proposal; there is no consensus or judgment on the validity of the transactions.

Before a formal VAT invoice is issued, DICE assures that A, B, and the U.K. and French tax authorities are aware of the transaction. There is time for risk analysis, and based on the Ceará and Rwandan experiences, the entire process can take less than three seconds. AI can spot high-risk transactions, which can be delayed or blocked by the authorities.

[25] Brazil's system uses a centralized federal data center to coordinate cross-border transactions of the state-level consumption tax, which is imposed with cross-border adjustments at different rates in each of the 26 subnational states. It contemplates replacing paper tax and accounting books and documents with electronic versions for which legal validity is confirmed with a digital signature. Digital documents are given legal precedence over paper replicas. *See* Newton Oller de Mello et al., ''The Evolution of Electronic Tax Documents in Latin America,'' 13th World Scientific and Engineering Academy and Society (WSEAS) International Conference on Systems (2009); and de Mello et al., ''The Implementation of the Electronic Tax Documents in Brazil as a Tool to Fight Tax Evasion,'' 13th WSEAS International Conference on Systems (2009).

[26] Ainsworth and Todorov, ''Rwanda — Cutting Edge VAT Compliance,'' 46 *CCH Global Tax Weekly* 5 (Sept. 26, 2013).

[27] Gahiji Innocent, ''Billing Machines Increase Tax Collection by 16 [Percent],'' *News of Rwanda*, Sept. 18, 2014 (citing comments by Revenue Authority Commissioner Richard Tushabe, who attributes the revenue increase both to more successful audits and to increased voluntary compliance because of the adoption of the new regime).

[28] Ainsworth and Todorov, ''Plugging the Leaks in the East African Community's VATs,'' *Tax Notes Int'l*, Nov. 11, 2013, p. 561.

[29] Maureen Odunga, ''Dar, Kigali for One Revenue Center,'' *Daily News*, July 2, 2016.

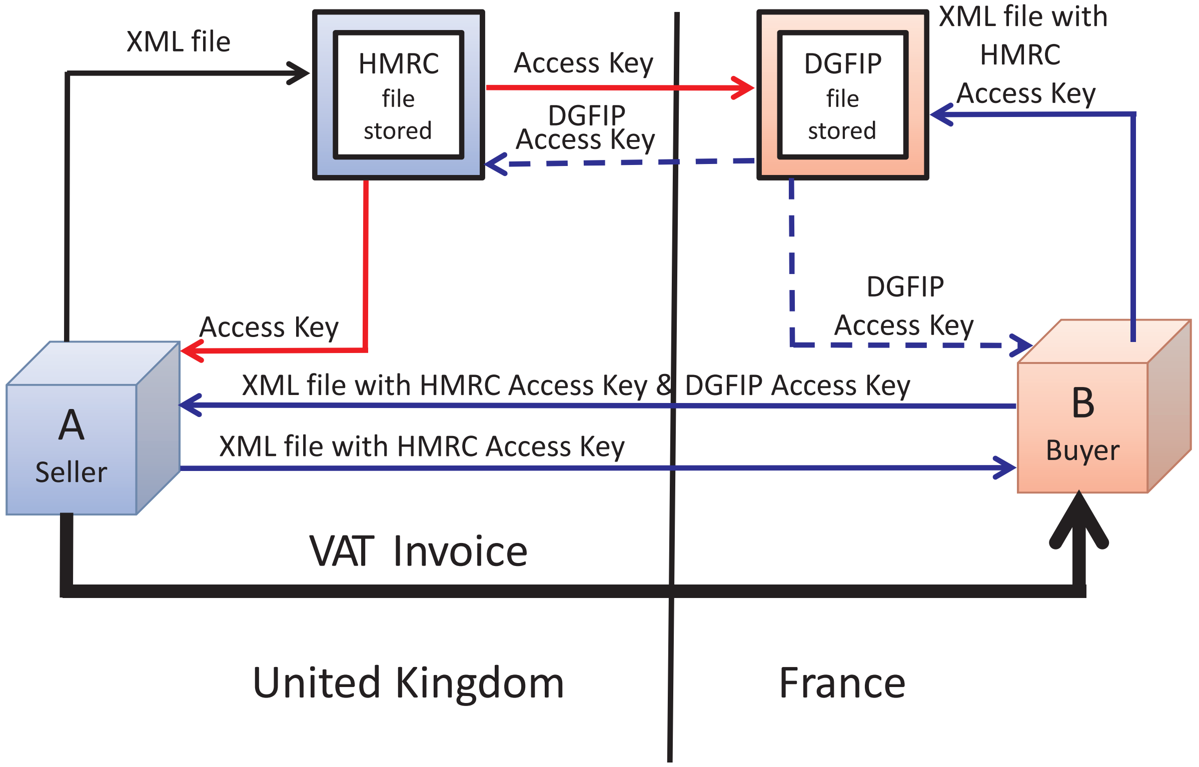
[30] Ainsworth and Todorov, *supra* note 28.

[31] Ainsworth, ''Phishing and VAT Fraud in CO_2 Permits: The Digital Invoice Customs Exchange Solution,'' *Tax Notes Int'l*, Jan. 26, 2015, p. 357.

[32] Personal communication with Paul Lindenfelzer, SmartCloud VP Sales and Operations (July 7, 2016).

[33] Niki Wiles, ''The Radical Potential of Blockchain Technology,'' London Futurist presentation (June 7, 2015); and Marc Pilkington, ''Blockchain Technology: Principles and Applications'' (2015).

Figure 2. Summary Figures 1-4



Note: This figure is reprinted from Ainsworth, "Stopping EU VAT Fraud With a Third Invoicing Directive," *Tax Notes Int'l*, Aug. 5, 2013, p. 545.

East African Community

The proposal drafted for the EAC was more flexible and did not presume multiple data centers. The intent was to allow for the possibility that the EAC might consider setting up a single central data center (closely following the Brazilian model) that would facilitate DICE oversight for the whole EAC. As a result, the customs exchange in the proposal is between member states.[34] The same submission of digitally signed XML files, encrypted data, and access keys shared among the parties are replicated. Local tax authorities pass encrypted data to the customs exchange, from where it is directly observable by parties with appropriate access keys. (See Figure 3.)

It seemed unlikely that a single data center would be workable for the EAC in the short term. The EAC headquarters are in Tanzania, which has been slow to fully politically integrate into the EAC. Tanzania was reportedly considering a separate arrangement with the Democratic Republic of Congo and Burundi.[35] By 2015, however, when Tanzania's president because the rotational EAC chair, it appeared there was progress in favor of integration.

The single data center for multiple jurisdictions might work in Nigeria, which like Brazil has a large federal tax presence coordinating local VAT compliance.[36] It might also work in the Gulf Cooperation Council (GCC), which is moving toward the adoption of a uniform 5 percent VAT by 2018.

A unified GCC data center in Riyadh coordinates customs for the council. There is coordination of data transfers, and through a direct transfer mechanism, duties collected in one GCC jurisdiction on goods destined for another are automatically transferred to the appropriate government.[37] One VAT scholar has said

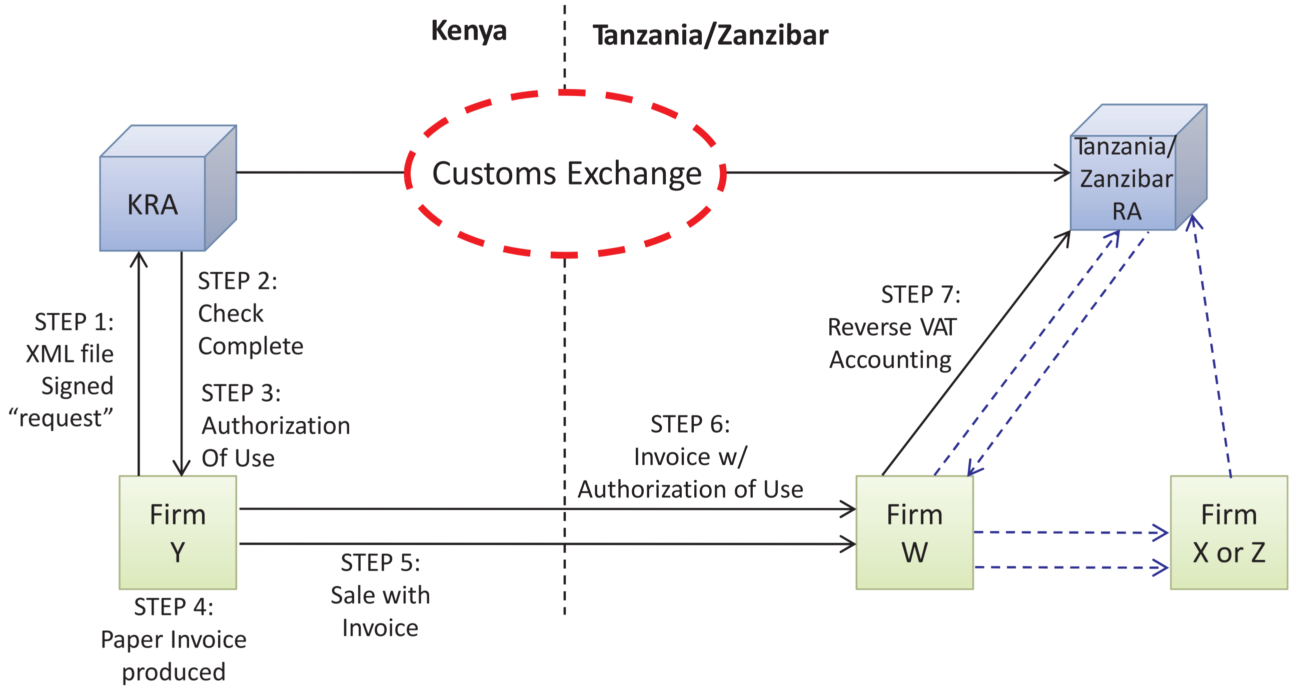
[34] Ainsworth and Todorov, *supra* note 28, at 579.

[35] "Tanzania Seeks New Partners Outside of EAC," *Daily Nation* (Oct. 31, 2013).

[36] James Alm and Jameson Boex, "An Overview of Intergovernmental Fiscal Relations and Sub-national Public Finance in Nigeria," Georgia State University, International Studies Program Working Paper 02-1 (Jan. 2002); and Olaoye Clement Olatunji, "A Review of Value Added Tax (VAT) Administration in Nigeria," 3 *Int'l Bus. Mgmt.* 61.

[37] Mohammed al-Hilali, "Immediate Sending of Data Transfers of Customs Duties Between the GCC," Aleqt.

Figure 3. Kenya and Tanzania/Zanzibar Customs Exchange


Kenya
Tanzania/Zanzibar
KRA
Customs Exchange
Tanzania/ Zanzibar RA
STEP 1: XML file Signed "request"
STEP 2: Check Complete
STEP 3: Authorization Of Use
STEP 7: Reverse VAT Accounting
STEP 6: Invoice w/ Authorization of Use
Firm Y
Firm W
Firm X or Z
STEP 4: Paper Invoice produced
STEP 5: Sale with Invoice

Note: This figure is reprinted from Ainsworth and Goran Todorov, "Plugging the Leaks in the East African Community's VATs," *Tax Notes Int'l*, Nov. 11, 2013, p. 561.

he anticipates that at least initially, customs will oversee the tax in the GCC.[38] As a result, a single centralized data center for VAT might be adopted through close work with customs.[39]

DICE on Blockchain

Blockchain is a revolutionary improvement on any centralized data system.[40] Tax administrations are inherently based on centralized repositories of taxpayer data and are prime candidates for the kinds of efficiency improvements that come through blockchain. That is particularly the case for transaction taxes, and even more so for a VAT fraud prevention application, like DICE, which relies on a real-time exchange of encrypted data.

For a VAT blockchain-run network that would substantially reduce cross-border frauds like MTIC and MTEC, an economic community would need a computer network, a network protocol, and a consensus mechanism. Each product or service traded would have its own distinct ledger of transactions showing the original and current owners, as well as each intermediary along the way. Each verified transaction of that supply would constitute a new block added to the ledger. It would be irrevocably tied to all previous blocks to create a blockchain.

There would be a verified history of VAT ownership, with validated transactions all along the chain. If the nodes in the network did not verify a transaction, a valid VAT invoice could not be issued. In other words, the seller would not be entitled to collect VAT from a buyer, and a buyer would not be allowed to deduct VAT paid. No change would be permitted in the ledger. In an intra-Community context, the seller would not be allowed to zero rate his sale and apply for a refund.

Computer Network

The computer network provides stability and security. Each computer is called a node. Blockchain is secure because there are a multitude of nodes in the system, which provides fault tolerance. Because each node

[38] Personal email communication (June 8, 2016) with Musaad Fahad Alwohaibi, an SJD candidate at the University of Florida Levin College of Law.

[39] Ehtisham Ahmad, ''Institutions, Political Economy, and Timing of a VAT; Options for Dubai and the UAE,'' in *Fiscal Reform in the Middle East — VAT in the Gulf Cooperation Council* 283, 288-292 (2010).

[40] Davidson et al., *supra* note 10 (blockchain provides better security, faster transactions, and is much cheaper than centralized data systems); Gideon Greenspan, ''Blockchains v. Centralized Databases,'' MultChain (Mar. 17, 2016); and Wright and de Filippi, *supra* note 7.

is running the identical copy of the chain containing all items in the system, if any node is compromised (hacking, power failure, sabotage), all other nodes will maintain the true ledger.

The DICE blockchain is a permissive system. It cannot be a public system like bitcoin because the network will have access to confidential taxpayer information. The operators must be government appointed. A significant portion of the work performed by each node would be automated, much like it is in a bitcoin mining operation, but rather than solving complex mathematical problems, the AI would be performing calculations and associating data points as directed by programming prompts of trained VAT auditors. Each node would need to assess each proposed transaction and determine if the parties involved were likely to be compliant taxpayers.

Larger trading countries would be required to contribute more computers to the network than smaller ones because they place the most weight on the VAT system and should bear a proportionate share of the compliance burden.

Network Protocol

An example of an applicable network protocol is the Sawtooth Lake distributive ledger platform unveiled by Intel on April 7. Intel contributed Sawtooth Lake to the HyperLedger blockchain project. A tutorial is available to assist in implementing the code.[41]

According to Intel, the materials available for download are all that is needed to construct a fully functional digital asset exchange. The basic components are:

- a data model that captures the current state of the ledger;
- a language of transactions that change the ledger state; and
- a protocol to build consensus among participants around which transactions will be accepted by the ledger.

Consensus Mechanism

The consensus mechanism provides the critical verification component to blockchain. Its parameters determine how the network of nodes verifies additions to any block in the system.

Bitcoin uses proof of work to verify transactions, which requires a massive commitment of computing resources — is necessary in an open system. Proof of work will objectively verify transactions between unknown and even hostile participants. Private systems do not require the same level of resource commitment because other controls are in place to ensure accuracy.[42]

There is no universally acceptable consensus mechanism in blockchain,[43] which should be expected. Consensus mechanisms should not be all-purpose and should instead should tie directly to the problem being solved. For instance, developers of restricted blockchain technologies can choose less expensive consensus algorithms in which validation is not always difficult or costly for all users but instead is costly for attackers only when there is an attack.[44]

In a distributed VAT ledger, the consensus mechanism must be based on objective criteria that evaluate the risk of VAT fraud. Intel's approach to deriving workable consensus mechanisms in Sawtooth Lake might be followed.[45]

EU VAT Transactions on the Blockchain

Many advances have been made in permissive distributed ledger technology. Major technology companies are contributing to design and workability.[46] The time is ripe for an application of distributed ledger technology to the EU VAT, given the huge revenue losses to MTIC and MTEC frauds.

As described, under the rules, business-to-business (B2B) transactions, goods sold between member states are zero rated when they leave the seller's jurisdiction and will be subject to a reverse charge in the buyer's jurisdiction. Similar rules apply in cross-border B2B sales of services. Both the seller's jurisdiction, which will be required to issue a VAT refund to taxpayers making cross-border sales, and the buyer's jurisdiction, which will be required for VAT to be remitted following the cross-border acquisitions, have an interest in confirming the legitimacy of the transaction.

Assume an automobile manufacturer in France produces 100 cars for export that are sold domestically to A for €10,000 each. A agrees to let B in the Netherlands acquire 10 of those cars for €11,000 each. After import, B resells the cars to a dealer in the Netherlands who sells on to final Dutch consumers.

[41] *See* https://intelledger.github.io/introduction.html.

[42] Andrea Pinna and Wiebe Ruttenberg, ''Distributed Ledger Technologies in Securities Post-Trading — Revolution or Evolution?'' European Central Bank Occasional Paper Series, No. 172 (Apr. 2016), at 10-11.

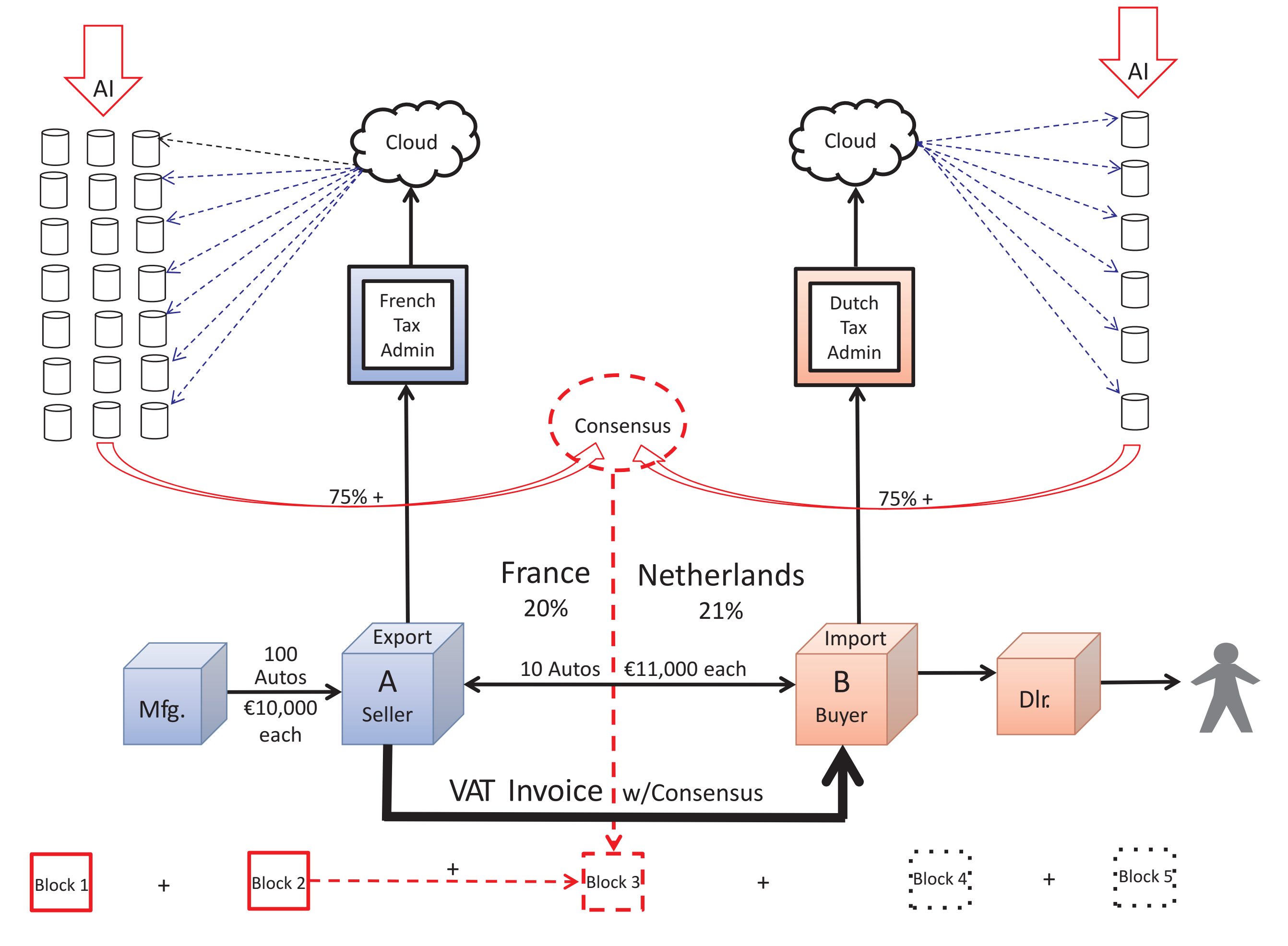
[43] *Id.*, at 14.

[44] *Id.*

[45] Intel created two new consensus protocols. One is a lottery protocol that builds on trusted execution environments provided by Intel's software guard extensions as a way to handle a large population of participants. The other is an adaptation of the Ripple and Stellar consensus protocols and serves to address the needs of applications that require immediate transaction finality.

[46] Kyt Dotson, ''Storj Beta Added to Azure BaaS Ecosystem, ShapeShift Hacked, Kraken Series B Investment,'' *Silicon Angle* (Apr. 13, 2016).

Figure 4. VAT Blockchain With 75 Percent Consensus Threshold



A distributed VAT ledger records the transactions for each of the cars from the manufacturer acquisition of materials to produce the 10 cars (block 1), which are transferred to A (block 2). The cross-border sale to B in the Netherlands is block 3. If consensus is reached, block 3 will be bound to block 2 in the same manner as block 2 was joined to block 1.

When A and B agree to the terms of the transaction, the rules of the distributed VAT ledger will require both parties to transmit that tentative agreement in an encrypted XML file to their respective tax administrations. From there, the agreement will pass to the cloud and then to the assigned nodes in each jurisdiction. Using AI, each node will be asked to approve or disapprove the proposed transaction.[47] If we further assume that the consensus threshold is set at 75 percent of the French nodes and 75 percent of the Dutch nodes, consensus would be registered (automatically) if approvals at that level were reached.

The invoice is the most critical VAT document. A uniform EU law change is needed to require that every valid VAT invoice display a digital fingerprint derived through the VAT blockchain consensus process. The fingerprint will identify that block 2 is permanently linked to block 1, and so on — the entire history of the commercial chain can be followed. A hand-held scanner connected to an approved tax auditing program would be all that is needed to immediately pull up the entire commercial chain for an item from a valid invoice.

To perform properly, each node must have immediate access to all standard invoice-level data about both parties and must be able to conduct AI-facilitated risk analysis. Because they are government nodes, each will have access to numerous public and private databases (as an auditor would). Statistical anomalies would be

[47] SmartCloud performs risk analysis for 60,000 taxpayers, handling 2 million transactions per day. AI of that quality installed at each node could more than handle the commercial transactions on a DICE blockchain. Lindenfelzer, *supra* note 32.

identified in real time, and authorities would be alerted. AI would move (or be directed) through available data points, and approaches preferred by node managers would guide the analysis. Some examples of points of inquiry include whether the prices charged are below market, whether the goods are adequately insured, and whether the buyer or seller is a newly registered taxpayer with insufficient capital to engage in transactions like those proposed.[48]

Conclusion

As with the original DICE proposal, putting invoice data into a blockchain will not eliminate the first instance of MTIC/MTEC fraud in a fraud chain but it should detect in real time any efforts to continue the fraud.

Tax administrations have limited resources, and efforts to stop MTIC/MTEC frauds are consuming huge amounts of time and effort. A blockchained DICE system could alter how tax authorities approach the detection of MTIC/MTEC fraud. That kind of regime would prompt intensive domestic data gathering, frequent record updating, and frequent accuracy checks of local taxpayers — a dramatic change from current efforts. Audit and investigation are retrospective and can result in massive global searches for largely foreign fraudsters who set up shell companies to carry out local frauds and then flee overseas.

In a blockchain regime, there is an enforcement premium in having comprehensive commercial databases. Inspection teams should spend significant amounts of time visiting new taxpayers and collecting (and confirming) data on business locations, types and quantities of trades, financial relationships, and employee count. Most of that information is already available in various government channels, but it must be readily accessible by the AI programs. In jurisdictions where databases are weak, the blockchain will drive change.

The beauty of blockchain is that it is trustless: Participants do not have to trust each other to use it with confidence. It ‘‘lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority’’[49] — precisely what is needed to combat MTIC/MTEC frauds. ◆

[48] For other examples, see the due diligence requirements listed in HM Revenue and Customs, ‘‘VAT Notice 726: Joint and Several Liability for Unpaid VAT’’ (Apr. 2, 2008).

[49] *The Economist*, *supra* note 9.