

BLOCKCHAIN (DISTRIBUTED LEDGER TECHNOLOGY) SOLVES VAT FRAUD

Boston University School of Law
Law & Economics Working Paper No. 16-41

Richard T. Ainsworth
Boston University School of Law

Andrew Shact
VP Tax and Treasury, Mimecast

This paper can be downloaded without charge at:

<http://www.bu.edu/law/faculty-scholarship/working-paper-series/>

BLOCKCHAIN (DISTRIBUTED LEDGER TECHNOLOGY)

SOLVES

VAT FRAUD¹

Richard T. Ainsworth
Andrew Shact

At the World Economic Forum more than 800 executive and technology experts were asked when they thought a particular “tipping point” would be reached – when would we see a government collect tax with blockchain? The agreed date was 2023 (on average). A full 73% of the respondents however, expected the tipping point to have been reached by 2025.²

The survey did not ask the experts to name the tax, or the jurisdiction. So, we do not know if this group of executives expect blockchain to be used to collect estate taxes,³ wage withholdings for personal income tax,⁴ corporate income tax, the retail sales tax, or the value added tax⁵ (VAT)? We also do not know in which jurisdiction we should expect to see this change.

¹ The lead author would like to thank his VAT class at NYU’s Graduate Tax Program during the Spring Term 2016 for engaging him in a discussion of blockchain during his presentation on MTIC fraud and the DICE solution. I confess that I knew very little about blockchain before this class engaged me on it, and feel I learned as much from them as they did from me at this juncture. We engaged in a very dynamic VAT policy dialogue that was always inspiring. Productive discussions continued with Andrew Shact, VP Tax and Treasury at Mimecast.

² Kimberly Johnson, *So, What Is Blockchain?* WSJ (June 20, 2016) at R6 in Journal Report: CFO Network.

³ Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, (March 12, 2015) available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 at 12:

The technology [of blockchain] could be employed to create smart contracts that automatically check the state death registries and allocate assets from a testator’s estate, send applicable taxes to government agencies without the need of administering the will through probate.

⁴ Francois Badenhurst, *Blockchain Pegged as UK’s Tax Future*, ACCOUNTINGWEB (January 27, 2016) <http://www.accountingweb.co.uk/tech/tech-pulse/blockchain-pegged-as-uks-tax-future> (suggesting that blockchain would be ideal for delivering government services in the personal tax account).

⁵ UK Government Office for Science, *Distributed Ledger Technology: Beyond block chain* (2016) available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. The discussion in the VAT portion of this document focuses on efficiency gains in government auditing, and recommends the development of an ...

... EU-wide series of VAT standards and protocols [that] would enable DLT to be deployed across Europe, with unilateral alignment of all VAT accounting transactions, from invoices to bank receipts. The system could include smart contracts designed to outsmart the tax quasi-compliant economy, which would also help to address the various threshold differences in VAT applicability across EU member states.

With machine-learning devices reading the EU’s VAT transactions in real time, erroneous transactions (including so-called carousel fraud) are far more likely to be spotted than by the current methods of auditing. Increasing traceability and transparency — including payment providers, banks and other financial institutions — would make the black-market economy more difficult to conceal. (70-71)

This paper argues that the EU VAT will be an early adopter, if not the earliest adopter of blockchain.⁶ There are a number of reasons why. Blockchain will bring substantial efficiencies to VAT collection. It will reduce costs, and build critical inter-governmental trust relationships. Most importantly, blockchain will immediately end revenue losses well in excess of €50 to €60 billion per year in missing trader intra-community fraud (MTIC).⁷

It is clear that the EU Commission is anxious to adopt new technologies in fraud prevention and detection. More effective data sharing and adoption of sophisticated artificial intelligence (AI) programs is critical in this effort. Member States need "... new models of sharing ... information ... enabling them to rapidly and more effectively identify and dismantle fraudulent networks."⁸

Blockchain will also be essential for making the EU Commission's April 2016 *Action Plan on VAT* work. Blockchain should be a critical part of the detailed legislative proposal (expected in 2017). This plan will bring in a "definitive VAT system" dealing with intra-EU cross-border trade, which will be based on taxation in the country of destination.⁹ This paper predicts that the EU will bring in the "definitive system" on the back of blockchain technology.

⁶ Melanie Swan, *Blockchain: Blueprint for a New Economy* O'Reilly Media Inc. (2015); Niki Wiles, *The Radical Potential of Blockchain Technology*, LONDON FUTURIST (JUNE 7, 2015) (considering blockchain in an economics of information, innovation and technological change event) available at: <https://www.youtube.com/watch?v=JMT0xwmFKIY>; Marc Pilkington, *Blockchain Technology: Principles and Applications*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660

Other approaches to blockchain look at it as an economics of money issue, largely because blockchain underpins Bitcoin and other crypto-currencies. Rainer Bohme, Nicolas Christin, Benjamin Edelman & Tyler Moore Bitcoin: Economics, Technology, Governance, 29 JOURNAL OF ECONOMIC PERSPECTIVES 213 (2015). Joshua Hendrickson, Thomas L. Hogan, & William J. Luther, *The Political Economy of Bitcoin*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2531518. Lawrence H. White, *The Market for Cryptocurrencies*, 35 CATO JOURNAL 383 (2015). Still others see it as an institutional or social technology for coordinating people and thus it is about a revolution in institution, organization, and governance. Sinclair Davidson, Primavera De Filippi & Jason Potts, *Economics of Blockchain*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751

⁷ 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 to €60 billion. Ernst & Young, *Implementing the "destination principle" to intra-EU B2B supplies of goods – Feasibility and economic evaluation study*, June 30, 2015, TAXUD/2013/DE/319 available at: http://ec.europa.eu/taxation_customs/resources/documents/common/publications/studies/ey_study_destination_principle.pdf. Note, the Ernst & Young 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 CO2 permits and VoIP. These are service-based frauds. Losses from these frauds far exceed those from goods.

⁸ EU Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, on an action plan on VAT: Towards a single EU VAT area – Time to decide COM(2016) 148 final (April 7, 2016) at 6, available at:

http://ec.europa.eu/taxation_customs/resources/documents/taxation/vat/action_plan/com_2016_148_en.pdf

As recognized by the European Court of Auditors, the tools of administrative cooperation between tax administrations are not being sufficiently exploited. Moreover, the implementation of the Eurofisc was not ambitious enough. We therefore need to *move from the existing cooperation models based on Member States exchanging information to new models of sharing and jointly analyzing information* and acting together. Member states should benefit from a risk management capacity at EU level, enabling them to rapidly and more effectively identify and dismantle fraudulent networks. (emphasis added)

⁹ EU Commission, Taxation and Customs Union, *Action Plan on VAT* (April 7, 2016) available at: http://ec.europa.eu/taxation_customs/taxation/vat/action_plan/index_en.htm

BLOCKCHAIN

Blockchain technology creates a robust, secure, transparent *distributive* ledger.¹⁰ The technique is revolutionary. Blockchain is a software protocol based on cryptography. It was devised in 2008, and was announced simultaneously with its most famous application – Bitcoin.¹¹

Bitcoin (the application) is often confused with blockchain (the technology). Bitcoin is only one application of blockchain technology. Ledger entries in the Bitcoin application are the Bitcoins generated by the Bitcoin protocol. However, distributive ledgers are not limited to cryptocurrencies. They can replace any centralized ledger system that coordinates valuable information.¹² When it is deployed, blockchain is highly disruptive to legacy systems.

Blockchain technology is *trustless*.¹³ It 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 help it negotiate (exchange) value. Instead of trusted intermediaries, blockchain uses powerful consensus mechanisms with cryptoeconomic incentives to verify the authenticity of transactions in the database.¹⁴ Depending on the application this incentive mechanism can change.¹⁵ This consensus mechanism makes the database safe (highly *trustworthy*) even in the presence of

¹⁰ A ledger, as used in this sentence and in this field generally, means a value recording and transfer system. Simply stated, a ledger is an accounting tool that keeps track of who owns what. The ledger itself is a very old technology that has not changed much since its development by the Venetian Republic in the 15th century. Ledgers have long been digitized (in the 20th century), but it was only with blockchain that they have been *decentralized*. Prior to 2008 ledgers were only understood as *centralized*.

¹¹ Satoshi Nakamoto, Bitcoin, *A peer-to-peer electronic cash system* (2008) available at: <https://bitcoin.org/bitcoin.pdf> (note: Satoshi Nakamoto is a pseudonym).

¹² Wright & De Filippi, *Decentralized Blockchain Technology* supra note 3 at 4-8.

¹³ The trust element is very important to the adoption of blockchain in tax compliance areas. It needs to be stressed that trusting the blockchain technology is different than trusting Bitcoin. Europol contends that it is not blockchain, but the "... Bitcoin [application that] is establishing itself as the single common currency for cybercriminals within the EU." Europol, 2015 INTERNET ORGANIZE CRIME THREAT ASSESSMENT, *Key Findings* available at: <https://www.europol.europa.eu/iocta/2015/key-findings.html>

¹⁴ Tim Swanson, *Great Wall of Numbers Cryptoeconomics for beginners and experts alike*, citing Vlad Zamfir of the Ethereum project at the Cryptocurrency Research Group conference (brainstorming session) on Cryptoeconomics as posted January 30, 2015 at: <http://www.ofnumbers.com/2015/01/30/cryptoeconomics-for-beginners-and-experts-alike/>. 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.

¹⁵ Cryptoeconomic incentives are most strongly associated with cryptocurrency systems. Bitcoin *mining* is such an incentive system. This is because Bitcoin uses pseudonymous and anonymous nodes to validate transactions, whereas a basic distributive ledger that engage entities with legal identities (banks, financial institutions, government agencies) will use "permissioned" nodes to validate transactions. This proposal of DICE on a blockchain uses permissioned nodes. For this reason, a basic distributive ledger is able to host off-chain assets (smart contracts) due to their authenticated, permissioned approach to validation. Tim Swanson, *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger System* (April 6, 2016) available at: <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>.

powerful or hostile third parties trying to manipulate the registry. For this reason, *The Economist* called blockchain, “The Trust Machine.”¹⁶

Only recently have decentralized, distributive ledgers been possible. Advances in technology, computing capacity, and connectivity (post-2000) have made this happen. Replacing very expensive *centralized ledgers* with *decentralized distributive ledgers* captures huge cost savings and efficiencies.¹⁷ Decentralized distributive ledgers ride three exponentially declining cost curves:

1. *Moore’s Law*: the cost of processing digital information (speed), halves every 18 months;¹⁸
2. *Kryder’s Law*: the cost of storing digital information (memory) halves every 12 months;¹⁹
3. *Nielson’s Law*: the cost of shipping digital information (bandwidth) halves every 24 months.²⁰

Bitcoin’s Blockchain

A Bitcoin is a digital asset that is acquired in exchange for other currencies, goods or services. The coins themselves are (originally) created as a reward for payment processing work in which users volunteer computer capacity to verify and record other individual’s transactions. This activity is called *mining*.²¹

Bitcoin is a payment system utilizing open source software.²² The system is peer-to-peer. Transactions take place between users directly. There is no intermediary (bank or other trusted third party).

Transactions are verified by network nodes, and recorded in a public distributed ledger where the Bitcoin itself is the unit of account. This is the blockchain. There is no central depository of Bitcoins. There is no administrator. Bitcoin is the world’s first decentralized digital currency.

¹⁶ THE ECONOMIST, *The Promise of Blockchain: The Trust Machine* (October 31, 2015) available at: <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>.

¹⁷ Sinclair Davidson, Primavera De Philippi & Jason Potts, *Economics of Blockchain* (March 8, 2016) available at: <http://ssrn.com/abstract=2744751>

¹⁸ Gordon E. Moore, Cramming More Components onto Integrated Circuits, Proceedings of the IEEE, Vol. 86, No. 1, January 1998) reprinting the same title from Electronics, 114-117 (April 19, 1965) available at: <http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf>. Mr. Moore is the founder of Intel and Fairchild Semiconductor.

¹⁹ Mark Kryder, *Kryder’s Law*, SCIENTIFIC AMERICAN (August 2005) available (as a reprint) at: <https://web.archive.org/web/20060329004626/http://www.sciam.com/article.cfm?chanID=sa006&colID=30&articleID=000B0C22-0805-12D8-BDFD83414B7F0000>. Mr Kryder was the senior Vice President of Research and the Chief Technology Officer at Seagate Corp.

²⁰ Jakob Nielson, *Nielson’s Law of Internet Bandwidth*, NIELSON NORMAL GROUP <https://www.nngroup.com/articles/law-of-bandwidth/>. Mr. Nielson was an engineer at Sun Microsystems.

²¹ The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. (page 4) Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

²² Open source software is computer software where its source code is made available (with a license) in which the copyright holder provides the right to study, change, and distribute the software to anyone and for any purpose.

The novelty of Bitcoin's blockchain is that it is a public ledger that is maintained by a network of communicating nodes running the Bitcoin software. A transaction will be constructed in the form of "X sends Y number of Bitcoins to Z." Network nodes receive this transaction and if they validate it the transaction will be added to *their copy* of the ledger. This copy is then broadcast to the other nodes. Approximately six times per hour a new group of accepted transactions (a block in the blockchain) is created. This "block" is what is added to the "chain" that comprises the "blockchain."

Owning and spending Bitcoins requires an individual to have a specific address. A payer must digitally sign a transaction with a private key.²³ If the private key is lost, the Bitcoin network will not recognize any other evidence of ownership.²⁴

Bitcoin transactions must have one or more inputs. For the transaction to be valid, every input must be an *unspent output* of a previous transaction. Every input must be digitally signed.²⁵ (In cases of multiple inputs, the Bitcoin system is simply indicating that multiple coins are being used to consummate a single transaction. The same is true in reverse, for a transaction with multiple outputs. Multiple payments can be made through the same transaction.)²⁶

Bitcoin uses a *public* (as opposed to a *private*) decentralized ledger. The term *public* is used because this ledger is accessible by every internet user. Anyone can participate in the verification process and determine which blocks can be added to the chain (the *mining* process).²⁷ The consensus mechanism is *proof-of-work*. "In the case of Bitcoin, the longest chain – the chain with the most proof-of-work – is considered to be the valid ledger."²⁸

Terminology can be confusing. For example, different terminology (different from *public* v. *private*) is used by the European Central Bank (ECB) to draw the same distinctions about blockchain. The ECB is considering blockchain for post trading activities in securities. The ECB rejects *unrestricted* (i.e., *public*) ledgers, and prefers *restricted* (i.e., *private*) ledgers in the

²³ Cryptographic systems use a pair of keys, one of which is public and can be shared widely, and the other of which is private and known only to the owner. Using a public key a message can be authenticated as originating with a holder of the paired private key. Additionally, encrypting a message with a public key will assure that only the holder of the paired private key can decrypt the message. Public-key cryptographic systems rely on cryptographic algorithms based on mathematical problems that currently admit no efficient solution.

²⁴ CBS-DC, *Man Throws Away 7,500 Bitcoins, Now Worth \$7.5 million* (November 29, 2013) available at: <http://washington.cbslocal.com/2013/11/29/man-throws-away-7500-bitcoins-now-worth-7-5-million/>

²⁵ See the diagram at page 2 in Satoshi Nakamoto, *Bitcoin, A peer-to-peer electronic cash system* (2008) supra note 11.

²⁶ As with a transaction in real currency, if the sum of the inputs (cash in your pocket) exceeds the sum of the outputs (funds needed to make a purchase), the difference is returned to the payer in the form of an additional output.

²⁷ Vitalik Buterin, *On Public and Private Blockchain* ETHEREUM BLOG (August 7, 2015) available at: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

²⁸ Tim Swanson, *Consensus-as-a-Service: a brief report on the emergence of permissioned, distributed ledger systems* (working paper, April 6, 2015) at 4, available at: <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>

securities field.²⁹ Other writers employ still different terminology. They distinguish between *permissioned* (i.e., *private*) and *unpermissioned* (i.e., *public*) distributive ledgers.³⁰ They do this to bring into sharp relief the use of white lists (or black list) of users, who are identified through KYB (know your bank) or KYC (know your customer) procedures. This process is common in traditional finance. Among all of these writers it is clear that *private, restricted, or permissioned* distributed ledgers work best in a governmental context.³¹

Mining is record-keeping. 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. The Bitcoin blockchain uses the SHA-256 hashing algorithm to *chain* the new block to the previous block.³²

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. *Blockchain Info* records Bitcoin's *Difficulty History* for proof-of-work and it indicates (for example) that from March 1, 2014 to March 1, 2015 the number of calculations a miner had to perform before creating a new block increased from 16.4 quintillion to 200.5 quintillion.³³

This expense of time, computational resources, and electricity is problematical for Bitcoin's *public* distributed decentralized ledger. It has encouraged developers to search for alternate validation systems. Proof-of-stake and proof-of-identity are two of the alternate consensus processes identified. They are well suited for *private (restricted, or permissioned)* distributed ledgers. The European Central Bank indicates:

A second type of validation system is proof-of-stake (PoS) consensus process. This assigns shares of validation rights to users according to their stake in the system ... or the reputation of the validator in a restricted DLT (known as proof-of-identity (PoI)).

²⁹ European Central Bank, *Distributed Ledger Technologies in Securities Post-trading: Revolution or Evolution?* OCCASIONAL PAPER SERIES, No. 172 (April 2016) available at:

<https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf>

³⁰ Tim Swanson, *supra* note 28, appears to have first use the expression "*permissioned*."

³¹ Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* (December 2015) at 16-24, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 (discussing the difference between permissioned and un-permissioned distributive ledgers and opting strongly for permissioned ledgers in the government sphere).

³² Andreas M. Antonopolous, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES at Chapter 8: *Mining and Consensus* 175-216 (2015) (explaining that to be acceptable by the rest of the network each new block must contain a proof-of-work. The proof-of-work requires miners to find a number (called a nonce) such that when the block is hashed along with the nonce the result is numerically smaller than the network's *difficulty target*. The proof is easy for any node to verify, but very difficult to generate. For a secure cryptographic hash miners must try many different nonce values before meeting the difficulty target.)

³³ Blockchain Info, *Difficulty History* at:

https://blockchain.info/charts/difficulty?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

The varying specifications that DLTs have in terms of participation in the ledger can indirectly affect the efficiency of the network. Instead of requiring every participant to invest a vast amount of resources in the maintenance of the ledger, responsibility for maintenance can be left to participants who will act in good faith, knowing that illicit behavior would be punished and the truthful state of the ledger re-established by agreement between accountable participants. Developers of restricted blockchain technologies can thus choose to use less expensive consensus algorithms than those that are necessary in unrestricted DLTs. In this way, in restricted DLTs validation is not made artificially difficult or costly for all users, on an ongoing basis, but is instead made costly for the attackers, and only when there is an attack.³⁴

MTIC, VIES, & DICE

The VAT Information Exchange System (VIES) is a database solution to cross-border VAT fraud. VIES uses old technology. It employs multiple centralized data centers. A semi-automatic (frequently manual) data exchange process involved. Recently, VIES' largest concern has been missing trader intra-community (MTIC) fraud. Annually, MTIC costs the EU €50 billion in goods-based frauds, and possibly another €50 billion in services-based frauds.³⁵ Service-based frauds can be extra-community (MTEC).³⁶

The Digital Invoice Customs Exchange (DICE) was the outgrowth of an effort to improve the fraud prevention functionality of VIES by developing a more granular, more automated, more immediate exchange of invoice-level data. DICE is technology-intensive, but not technologically heavy. It 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 is shared automatically, and in advance of performance. It is shared among the jurisdictions and the taxpayers that are parties to a specific transaction. It allows local enforcement against local losses.

However, DICE requires that the EU adopt a Third Invoicing Directive. From a workability perspective Brazil's digital invoicing regime, *Sistema Publico de Escrituracao Digital* or Public System for Digital Accounting (SPED) 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.

DICE is not just another modification of the VIES. It requires fundamental modifications. Recapitulative statements and the current VIES can never provide real-time

³⁴ European Central Bank, *Distributed Ledger Technologies in Securities Post-trading: Revolution or Evolution?* Supra note 24 at 14.

³⁵ Europol, *SOCTA (Serious and Organized Crime Threat Assessment) 2013 – Public Version*, 27 (March 2013) (estimating MTIC losses at €100 billion annually).

³⁶ Richard T. Ainsworth, *VAT Fraud: The Tradable Services Problem*, 61 TAX NOTES INTERNATIONAL 217 (January 17, 2011) (discussing VAT fraud in tradable services, developing the concept of missing trader extra-community fraud and creating the acronym MTEC).

enforcement. An example of MTIC fraud helps to work through the operation of VIES and DICE. From here we can see how blockchain carries this analysis the next step forward.

MTIC Example

Assume that Firm “A” in the Netherlands agrees to sell a specific quantity of identified high-value goods to firm “B” in France. The price is set. The time and method of delivery are also agreed. In this *intra-community* supply Firm “A” will zero-rate this sale. It will file a return in the NL that seeks the return of all VAT paid to the NL (that is, it will seek recovery of the input VAT it paid on purchases related to this sales output). Firm “B” is expected to perform a reverse charge in France. That is, it will self-assess the French VAT on the goods it has purchased and record this transaction on its French return.³⁷

MTIC fraud would arise if Firm “B” does not perform the reverse charge, does not file an accurate French VAT return, does not remit the French VAT due, but nevertheless sells the goods on to Firm “C” in France with VAT collected on the new selling price. By not remitting the French VAT “Firm B” is a “missing trader.” The fraud is equal to the VAT charged on the onward sale. The French revenue authority needs to find “Firm B” quickly, as its owners are likely to leave the country.

The VIES system hopes to detect this fraud by sharing data among tax jurisdictions. Along with “Firm A’s” VAT return a recapitulative statement is filed with the Dutch tax authority. This statement provides a list of the cross-border entities “Firm A” has sold to, and an aggregate amount of sales per entity. The French tax administration can request this data when it performs an audit on “Firm B.”

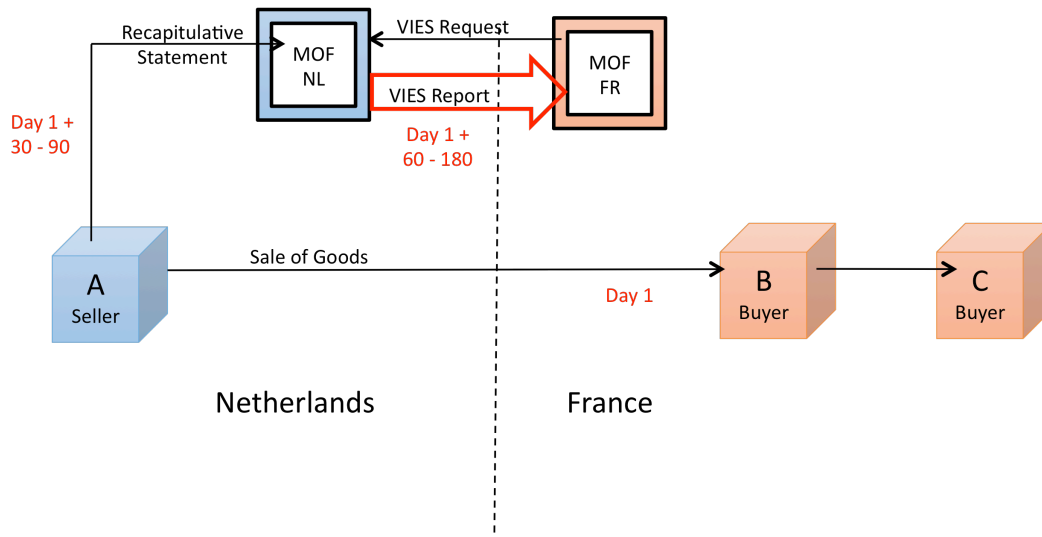
The timing of this data exchange is protracted. “Firm A’s” VAT return and recapitulative statement may be filed one, three or twelve months after the fraud transaction has occurred, depending on its Dutch filing status. Per regulation, the Dutch authorities must respond to the French request for this data within three months, although an expedited response (one month) is

³⁷ On November 28, 2006 the SIXTH COUNCIL DIRECTIVE of 17 May 1977 on the harmonization of the laws of the Member States relating to turnover tax – Common system of value added tax: uniform basis of assessment (77/388/EEC) 1977 O.J. (L 145) 1 – was repealed and replaced with the RECAST VAT DIRECTIVE (RVD), Council Directive 2006/112/EC on the Common system of value added tax, O.J. (L 347) 1. The texts are nearly identical. The intent was to rationalize the numbering of the articles.

Article 20 RVD [formerly Article 28a(3)] defines an intra-Community acquisition of goods as the right to dispose as owner of movable tangible property dispatched or transported to the person acquiring the goods by or on behalf of the vendor or the person acquiring the goods, in a Member State other than that in which the dispatch or transport of the goods began. Article 138(1) [formerly Article 28c(A)(a) 1st paragraph] requires the Member State making the supply to exempt the transaction (with full right of deduction) – sometimes called “zero rating.” Article 83 [formerly Article 28e(1) 1st paragraph] requires the Member State of acquisition to 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. Article 195 [formerly Article 28g(1)(f)] places 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.”

possible if the requested jurisdiction (the Netherlands) is already in possession of the information.³⁸ Figure 1 (below) illustrated this discussion.

Figure 1: Basic VIES Operation



The most obvious difficulties with this system are that: (a) it is *request based*, (b) it provides aggregate data not *invoice-level granular data*, and (c) the data exchange (VIES Report) is *delayed* at least two to six months after a suspect transaction has occurred. It is all too clear that MTIC frauds can be completed much faster than the VIES system can issue a report on it. For example, it took only 69 days for Sandeep Singh Dosanjh to complete a €41,501,591 MTIC fraud in CO2 permits.³⁹ VIES was totally inadequate to identify, much less stop Dosanjh.

Digital Invoice Customs Exchange (DICE)⁴⁰

Each of the previously published DICE proposals presumed the tax authorities worked with a centralized database. There were two permutations in these proposals depending upon whether the database contained transactional data *only from a single tax jurisdiction* (Rwanda and Ceará), or whether the single database is collecting tax data from *multiple jurisdictions in a community* (the Brazilian SPED).

³⁸ Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added taxation, 2010 O.J. (L-268) 1, at Art. 10, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:268:0001:0018:en:PDF>

³⁹ Richard T. Ainsworth, *VAT Fraud Mutation, Part 1: "Push" Missing Trader Fraud and Dosanjh*, 81 TAX NOTES INTERNATIONAL 535 (February 8, 2016).

⁴⁰ Richard T. Ainsworth & Goran Todorov, *Stopping VAT Fraud with DICE – Digital Invoice Customs Exchange*, 72 TAX NOTES INTERNATIONAL 637 (November 18, 2013).

Special problems are created when a number of tax jurisdictions are bound together in a community, but when each tax jurisdiction insists on keeping separate central databases of its own tax data (the EU is an example of this). 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 of the jurisdictions holds its own data centrally? Security systems are operating at a high level to protect the data, and as a result, processes and procedures to grant external access to this data are cumbersome and time consuming. The early DICE papers demonstrated how this process could be streamlined with encryption and sharing of public access keys. However, there is an even better way to accomplish the DICE objectives through decentralized databases or distributed ledgers.

Initial proposals – EU, Rwanda & Ceará

When DICE was first proposed, it addressed VIES/MTIC problems in the EU.⁴¹ The basic design incorporated elements of Brazil's successful digital invoicing regime, *Sistema Publico de Escrituracao Digital* or Public System for Digital Accounting (SPED) into a proposal for a Third Invoicing Directive.⁴² Brazil's SPED uses a centralized federal datacenter to coordinate cross-border transactions of the state-level consumption tax (ICMS) which is imposed with cross-border adjustments at different rates in each of the 26 sub-national states.⁴³

It was clear in that proposal that DICE could be used to solve both (a) frauds occurring within a single state (as in Rwanda & Ceará) as well as (b) frauds that occurred between states in a community, even when the relevant tax data might be stored in multiple, centralized databases.

DICE has been successfully implemented in Rwanda.⁴⁴ Revenue increased 16% in the first six months after adoption.⁴⁵ There is a potential community application for DICE in Africa.

⁴¹ Richard T. Ainsworth, *Stopping EU VAT Fraud With a Third Invoicing Directive* 71 TAX NOTES INTERNATIONAL 545 (August 5, 2013).

⁴² SPED contemplates replacing paper tax and accounting books and documents with electronic versions where legal validity is confirmed with a digital signature. Once a firm begins to issue NF-e invoices, or CT-e electronic waybills paper replicas of these documents are not legally valid. Digital documents are given legal precedence over paper replicas. See: Newton Oller de Mello, Eduardo Mario Dias, Caio Fernando Fontana & Marcelo Alves Fernandez, *The Evolution of Electronic Tax Documents in Latin America*, PROCEEDINGS OF THE 13TH WORLD SCIENTIFIC AND ENGINEERING ACADEMY AND SOCIETY (WSEAS) INTERNATIONAL CONFERENCE ON SYSTEMS (2009) 449, 297, available at: <http://dl.acm.org/citation.cfm?id=1627575&picked=prox>; and Newton Oller de Mello, Eduardo Mario Dias, Caio Fernando Fontana & Marcelo Alves Fernandez, *The Implementation of the Electronic Tax Documents in Brazil as a Tool to Fight Tax Evasion*, PROCEEDINGS OF THE 13TH WORLD SCIENTIFIC AND ENGINEERING ACADEMY AND SOCIETY (WSEAS) INTERNATIONAL CONFERENCE ON SYSTEMS (2009) 449, 453, available at: <http://dl.acm.org/citation.cfm?id=1627575&picked=prox>

⁴³ *Impostos Sobre Circulação de Mercadorias e Prestação de Serviços* (ICMS). The ICMS is the state sales tax and the rate varies depending upon the industry and the State.

⁴⁴ Richard T. Ainsworth & Goran Todorov, Rwanda – Cutting Edge VAT Compliance 46 CCH Global Tax Weekly 5 (September 26, 2013).

⁴⁵ Gahiji Innocent, *Billing Machines Increase Tax Collection by 16%*, NEWS OF RWANDA (September 18, 2014) available at: <http://www.newsofrwanda.com/featured1/24681/billing-machines-increase-tax-collection-by-16/> (citing comments by the Commissioner of the Rwanda Revenue Authority, Richard Tushabe who attribute the

Several other members of the East African Community (EAC) are considering DICE, and as a result a separate proposal was crafted for the EAC.⁴⁶

In this context it was not (and still is not) clear how a single EAC database will be set up, however recent event suggest that Tanzania is open to adoption of a single centralized data center with Rwanda.⁴⁷ Thus, the EAC data structure could adopt either (a) a multi-jurisdictional DICE solution similar to what would work in the EU where each Member State keeps its own datacenter with data shared through encryption and exchange of access key, or it could be (b) a single centralized system similar to what works in the Brazilian SPED with a single datacenter collecting and coordinating data exchanges among all members.⁴⁸

Another fully developed, single state adoption of DICE is operational in the Brazilian state of Ceará. The Ceará application is particularly noteworthy as it includes a state-of-the-art artificial intelligence (AI) program set up by SmartCloud Inc. that scans all data streams for a real-time risk assessment.⁴⁹ SmartCloud Inc. is able to provide “immediate” risk analysis reports,⁵⁰ and will go back over data looking for fraud patterns continuously, as well as responding to specific system queries by trained auditors.⁵¹

DICE in Rwanda and Ceará operate on centralized ledgers.⁵² There are three well-recognized problems with centralized ledgers (see 1-3 below).⁵³ A fourth problem arises when

revenue increase both to more successful audits and to increased voluntary compliance because of the adoption of the new compliance regime).

⁴⁶ Richard T. Ainsworth & Goran Todorov, *Plugging the Leaks in the East African Community's VATs* 72 TAX NOTES INTERNATIONAL 561 (November 11, 2013).

⁴⁷ Maureen Odunga, *Dar, Kigali for one revenue center*, DAILY NEWS (July 2, 2016) available at: <http://dailynews.co.tz/index.php/home-news/51260-dar-kigali-for-one-revenue-centre> (indicating that at the 40th Dar es Salaam International Trade Fair (DITF) President Paul Kagame of Rwanda and President John Magufulu of Tanzania agreed to establish a single revenue collection center).

⁴⁸ Richard T. Ainsworth & Gordon Todorov, *Plugging the Leaks in the East African Community's VATs*, 72 TAX NOTES INTERNATIONAL 561 (November 11, 2013).

⁴⁹ Richard T. Ainsworth, *Phishing and VAT Fraud in CO2 Permits: The Digital Invoice Customs Exchange Solution*, 77 TAX NOTES INTERNATIONAL 357, 367 at n. 37 (January 27, 2015) (discussing DICE applications in the EU Energy market and comments from SmartCloud Inc.'s CEO on the AI system installed in Ceará and further explaining how this technology could be applied in other areas for fraud detection).

⁵⁰ Personal communication, Paul Lindenfelzer, Partner, VP Sales and Operations, SmartCloud, Inc., (Bedford, MA) July 7, 2016 (plindenfelzer@smartcloudinc.com) responding to:

QUESTION: How quickly does the SmartCloud Inc. return a risk analysis report?

ANSWER: As long as the information required to run the analysis is available, it can be “immediate = second”

⁵¹ Personal communication, Paul Lindenfelzer, Partner, VP Sales and Operations, SmartCloud Inc., (Bedford, MA) July 7, 2016 (plindenfelzer@smartcloudinc.com) responding to:

QUESTION: does the Brazil system continue to churn out risk analysis profiles AFTER the initial report? does it go back over the data it has looking for more patterns (automatically) or does someone have to query the system to get this?

ANSWER: It is a little of both but mainly the latter. Once a description of a pattern or situation has been described, the system will continue to evaluate the existence of such automatically.

⁵² In Rwanda's case the VAT is a national tax, and so is the database. The data center is at the Rwanda Revenue Authority (RRA) headquarters Kimihurura, in Kigali. In Ceará's case the tax is the state level ICMS, the database is state level, and it is overseen by the state tax administration in Fortaleza.

centralized ledgers are used in a VAT context (see 4 below). All of these problems are resolved when moving to distributed ledgers (blockchain):

1. A centralized ledger is a single point of failure for the whole system;
2. A centralized ledger is prone to corruption because it consolidates power;
3. A centralized ledger is inherently insecure, and ends up consuming huge amounts of resources to protect the data within it; and
4. A centralized ledger is inherently inadequate as a comprehensive VAT compliance mechanism. A single, jurisdictionally bound, database can never capture all relevant *transactional* data. Centralized ledgers by definition only store data from *taxpayers* within *their jurisdiction*. Exceptional measures must be in place whenever confidential data is imported from outside the jurisdiction.

The original DICE proposal sought to resolve the fourth problem area above for transactions occurring entirely within the EU. The solution advanced by DICE *could be* applied, for example, to transactions between the EU and Russia if Russia agreed, but that discussion was not entertained in the proposal, because such an arrangement was deemed unlikely.

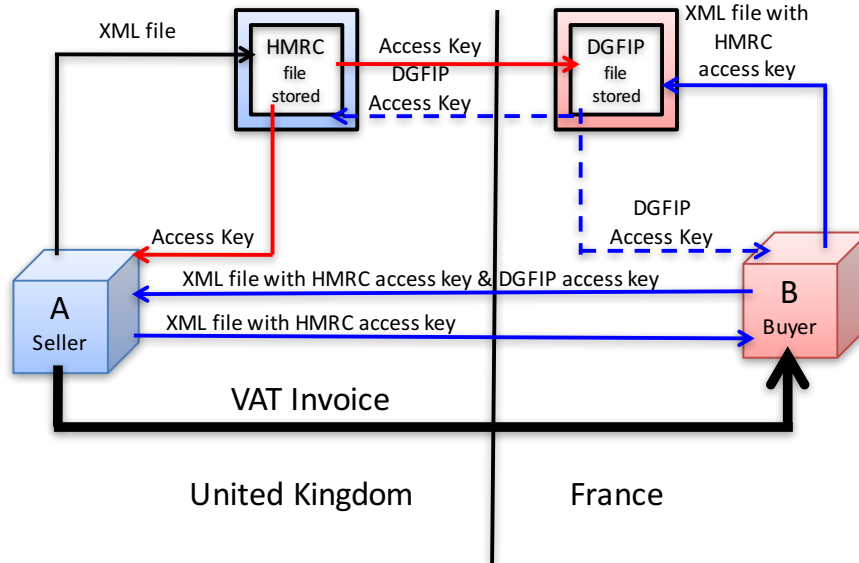
In this DICE proposal it was assumed that the EU would not accept a community-wide central database (in Brussels for example). It was also assumed that each EU Member State would insist on controlling and sharing data held within their own centralized database (largely) according to its own rules, and procedures.

As a result, in the EU DICE proposal there are assumed to be 28 independent centralized databases. The following diagram (Summary Figures 1-4, Complete Sequence) summarizes the data flows between a hypothetical “Seller A” in the UK and a hypothetical “Buyer B” in France. XML files are sent to separate (UK and French) datacenters, 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. This DICE proposal is a pure data exchange proposal. There is no consensus or judgment made on the validity of the transactions. See figure 2 (below).

⁵³ Niki Wiles, *The Radical Potential of Blockchain Technology*, LONDON FUTURIST (JUNE 7, 2015) available at: <https://www.youtube.com/watch?v=JMT0xwmFKIY>; Marc Pilkington, *Blockchain Technology: Principles and Applications*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660

Figure 2

Reprint: Summary Figures 1-4
 From 71 TNI 545, 552 (August 5, 2013)



Before a formal *VAT Invoice* issues, DICE assures that “Seller A,” “Buyer B,” HMRC in the UK, and the DGFIP in France are fully aware of the transaction. There is time for risk analysis. Based on the Ceará and Rwandan experiences, this entire process can take less than three seconds. Artificial intelligence (AI) can spot high-risk transactions. Suspect transaction can be delayed, or blocked by the authorities.

Second proposal – East African Community

The proposal drafted for the East African Community (EAC) was more flexible.⁵⁴ It did not presume multiple datacenters, as in the EU. The intent was to allow for the possibility that the East African Community might consider setting up a single central datacenter (closely following the Brazilian model), and this center would facilitate DICE oversight for the whole EAC.⁵⁵ As a result, the Customs Exchange is represented in that proposal sitting *between* Member States (Kenya and Tanzania/Zanzibar). See figure 3 (below), which re-prints the “Kenya and Tanzania/Zanzibar Customs Exchange” diagram from that proposal.⁵⁶

⁵⁴ Five countries make up the EAC: the Republics of Kenya, Uganda, the United Republic of Tanzania, Republic of Burundi, and the Republic of Rwanda. The headquarters are in Arusha, Tanzania.

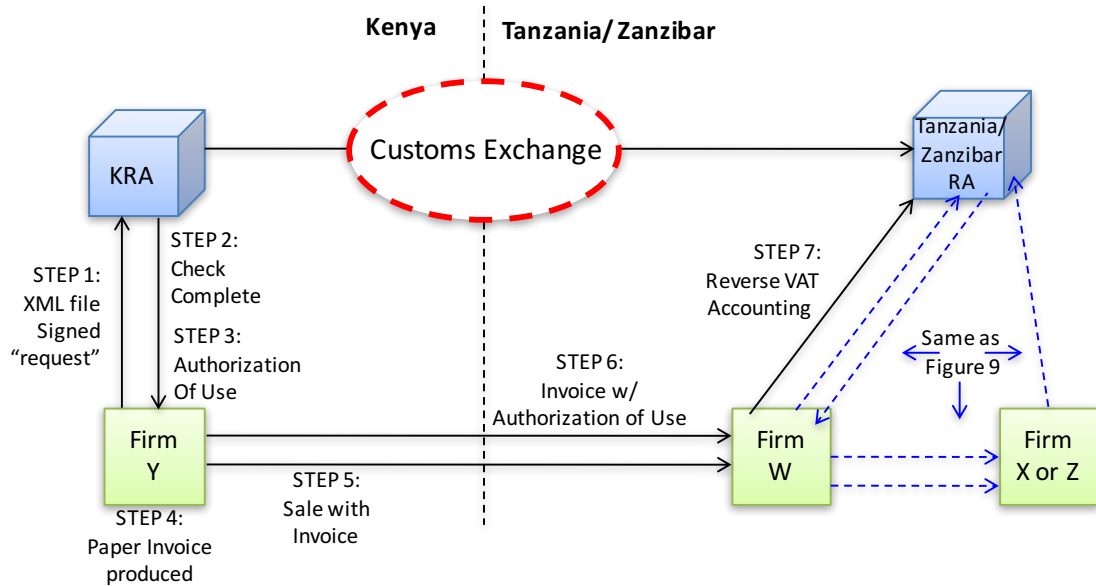
⁵⁵ There are indications that when VATs are introduced in the Gulf Cooperation Council (GCC) some time in 2018 involving the six Arabian countries of Saudi Arabia, the United Arab Emirates, Oman, Kuwait, Qatar, and Bahrain that a central data center would be considered.

⁵⁶ (November 11, 2013) 72 TNI 561, 579

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.

Figure 3

Reprint: Kenya and Tanzania/Zanzibar Customs Exchange
From 72 TNI 561, 579 (November 11, 2013)



It had seemed unlikely that a single central datacenter would be workable for the EAC in the short term. The EAC headquarters are in Tanzania, and recently Tanzania has been “going slow” with respect to a full political integration into the EAC. Tanzania was reportedly looking at “plan B,” which was a separate arrangement with the Democratic Republic of Congo and Burundi.⁵⁷ Although by 2015, when Tanzania’s president assumed the rotational chairmanship of the EAC, it appeared that there was progress in favor of integration. In 2016 it appears that this trend is still moving forward.

In an African context, the single data center for multiple jurisdictions model may be workable in Nigeria, which like Brazil has a large federal tax presence coordinating local VAT compliance.⁵⁸

⁵⁷ Xinhua, *Tanzania Seeks New Partners Outside of EAC*, DAILY NATION (October 31, 2013) available at: <http://www.nation.co.ke/news/africa/Tanzania-seeks-new-partners-outside-EAC/-/1066/2054870/-/taij9/-/index.html>

⁵⁸ James Alm & Jameson Boex, *An Overview of Intergovernmental Fiscal Relations and Sub-national Public Finance in Nigeria*, GEORGIA STATE UNIVERSITY, ANDREW YOUNG SCHOOL OF POLICY STUDIES, INTERNATIONAL STUDIES PROGRAM WORKING PAPER 02-1 (January 2002) available at: https://www.researchgate.net/publication/4737803_An_Overview_of_Intergovernmental_Fiscal_Relations_and_Sub

This single data center concept is design that may also work in the Gulf Cooperation Council (GCC). The GCC is comprised of six Middle Eastern countries (Saudi Arabia, Kuwait, the United Arab Emirates, Qatar, Bahrain and Oman). They are moving together toward the adoption of a uniform 5% VAT by 2018.

A single central database is a may be a likely outcome in the GCC. At the present time a unified datacenter, located in Riyadh, Saudi Arabia, coordinates customs for the six countries.⁵⁹ There is coordination of data transfers, and through a “direct transfer mechanism” duties collected in one GCC jurisdiction on goods destined for another GCC jurisdiction are automatically transferred to the appropriate government.⁶⁰ According to one of the few VAT scholars in the GCC, Mr. Musaad Fahad Alwohaibi,⁶¹ it is anticipated that at least initially customs will oversee the VAT in the GCC, and as a result a single centralized data center for VAT may be adopted through close work with customs.⁶²

DICE ON BLOCKCHAIN

Blockchain is a revolutionary improvement on any centralized data system.⁶³ Tax administrations are inherently based upon centralized repositories of taxpayer data. They are prime candidates for the kinds of efficiency improvements that come through blockchain. This

[national Public Finance in Nigeria](#); Olaoye Clement Olatunji, *A Review of Value Added Tax (VAT) Administration in Nigeria* 3 INTERNATIONAL BUSINESS MANAGEMENT 61 available at:

<http://docsdrive.com/pdfs/medwelljournals/ibm/2009/61-68.pdf>

⁵⁹ Customs Information Center, General Secretariat of the GCC in Riyadh, Saudi Arabia. See:

<http://www.gccic.org/cic/en/default.aspx>

⁶⁰ Mohammed al-Hilali, *Immediate Sending of Data Transfers of Customs Duties between the GCC*, ALEQT, available at: http://www.aleqt.com/2016/02/21/article_1032102.html

⁶¹ Musaad Fahad Alwohaibi is a Saudi national who specializes in VAT, and is candidate for the SJD at the Levin College of Law, University of Florida. Personal e-mail communication (on file with author) m_wohaibi@hotmail.com.

⁶² Ehtisham Ahmad, *Institutions, political economy, and timing of a VAT; options for Dubai and the UAE*, in Ehtisham Ahmad & Abdulrazak Al Faris, *FISCAL REFORM IN THE MIDDLE EAST – VAT IN THE GULF COOPERATION COUNCIL* (2010) at 283, 288-292 (discussing VAT administration options where the UAE is considered as a microcosm of the GCC with opportunities to have several VAT administrations (and related data centers) or a single VAT administration (with a single data center), but in all cases a close relationship with customs is assured because of the transactional nature of the VAT, with an eventual migration to an independent VAT administration anticipated under the UK model).

⁶³ Sinclair Davidson, Primavera De Philippi & Jason Potts, *Economics of Blockchain* (March 8, 2016) available at: <http://ssrn.com/abstract=2744751> (approaching blockchain from an economic perspective Davidson, De Philippi & Potts argue that blockchain provides better security, faster transactions and much lower cost than centralized data systems, and consequently at 3 indicate that blockchain will “disrupt any centralized system that coordinates valuable information.”); Gideon Greenspan, *Blockchains v. Centralized Databases* MULTICHAIN (March 17, 2016) available at: <http://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/> (comparing blockchain and centralized databases with an assessment of system advantage: (1) disintermediation – blockchain advantage; (2) confidentiality – centralized databases advantage; (3) robustness – blockchain advantage; (4) performance – centralized databases advantage; Aaron Wright & Primavera De Philippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, (March 12, 2015) available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (comparing the disruptive potential of blockchain to the disruption power of the internet over older communication systems and the need to develop regulatory structures to deal with this new reality).

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.

An economic community (the EU, the EAC, or the GCC) would need three things to set up a “VAT Network” run on blockchain technology that would substantially reduce (if not eliminate) cross-border frauds like MTIC and MTEC. The elements needed are:

- A network of computers;
- A network protocol; and
- A consensus mechanism.

Each product or service traded would have its own distinct ledger of transactions showing who originally owned the supply, and who currently owned it (as well as each intermediary along the way that bought and sold it). Each verified transaction of that supply would constitute a new “block” added to the ledger. It would be irrevocably tied to all previous “blocks” in the ledger, thereby creating a blockchain.

There would be a verified history of VAT ownership, with validated transactions all along the chain. If the nodes in the network do not verify a transaction, then a valid VAT invoice cannot issue. 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.

The network of computers. 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. This provides “fault tolerance.” Because each node is running the identical copy of the chain containing all items in the system, if any node is compromised in any manner (hacking, power failure or deliberate sabotage) all other node will maintain the true ledger.

The DICE blockchain is a *permissive* system. It cannot be a *public*, or *un-restricted*, or *permissionless* system like Bitcoin uses, because the network of computers 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 in this case rather than solving complex mathematical problems the Artificial Intelligence (AI) employed would be performing calculation and associating data-points in a manner suggested by programming prompts of trained VAT auditors. Each node would need to assess each proposed transaction and determine (based on the data available) 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 trading countries. These countries are placing the most weight on the VAT system, and should bear a proportionate share of the compliance burden. For example, the German GDP (at €3,025 billion) is roughly ten times larger than the Austrian GDP (of €337.2 billion). This

would suggest that Germany would need to contribute 10x the number of computer nodes as would Austria.⁶⁴

Network protocol. A network protocol is how computers communicate with one another. In the blockchain context this is how the “nodes” transmit information among themselves.

An example of an applicable network protocol is the “Sawtooth Lake” distributive ledger platform unveiled by Intel on April 7, 2016. Intel contributed Sawtooth Lake to the HyperLedger blockchain project,⁶⁵ posting it that day to GitHub. A detailed information release accompanied the posting and outlines the major elements of Sawtooth Lake. A tutorial is available with the release to assist the implementation of the code.⁶⁶

According to Intel, the materials that were made available for download are all that is needed to construct a “fully functional” digital asset exchange right “out-of-the-box.” The basic components are:

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

Intel explains:

In Sawtooth Lake, the data model and transaction language are implemented in a “transaction family.” While we expect users to build custom transaction families that reflect the unique requirements of their ledgers, we provide three transaction families that are sufficient for building, testing and deploying a marketplace for digital assets:

- *EndPointRegistry* – a transaction family for registering ledger services.
- *IntegerKey* – A transaction family used for testing deployed ledgers.
- *MarketPlace* – A transaction family for buying, selling, and trading digital assets.

Consensus Mechanism. The consensus mechanism provides the critical verification component to blockchain. The parameters set for the consensus mechanism determines how the “network of nodes” verifies additions to any block in the system.

Bitcoin uses “proof of work” to verify transactions, which means that the nodes in the network run complicated algorithms to verify each transaction. There is a massive commitment of computing resources in “proof of work,” but this is necessary because Bitcoin is an open (or

⁶⁴ Eurostat, *Gross Domestic Product at Market Prices*, available at:

<http://ec.europa.eu/eurostat/tgm/refreshTableAction.do?tab=table&plugin=1&init=1&pcode=tec00001&language=en>

⁶⁵ The HyperLedger blockchain project is a collaborative effort created by the Linux Foundation to help establish an open, distributed ledger platform to “satisfy a variety of use cases across multiple industries to streamline business processes.” See: <https://www.hyperledger.org>

⁶⁶ Intel’s full posting is available at: <https://intelledger.github.io/introduction.html>

“permissionless”) system. Proof-of-work will objectively verify transactions between unknown and even hostile participants.

Permissioned systems do not require the same level of resource commitment. Other control measures are in place to assure accuracy.⁶⁷

There is no universally acceptable consensus mechanism in blockchain.⁶⁸ This should be expected. Consensus mechanism should not be all-purpose, they should tie directly to the problem being solved.

Developers of restricted [permissioned] blockchain technologies can thus choose less expensive consensus algorithms than those that are necessary in unrestricted DLTs. In this way, in restricted DLTs validation is not made artificially difficult or costly for all users, on an ongoing basis, but instead is made costly for attackers, and only when there is an attack.⁶⁹

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.⁷⁰

⁶⁷ Andrea Pinna & Wiebe Ruttenberg, *Distributed Ledger Technologies in Securities Post-Trading – Revolution or Evolution?* European Central Bank Occasional Paper Series, No. 172 (April 2016) at 10-11 indicates:

Restricted [permissioned] DLTs are closed systems whose members are identified and accountable entities. Ledger updates can only be proposed and validated by authorized participants. ... In a restricted distributed ledger the identity of participants is known, at least by its governance body. This implies that any wrongdoer can be identified and his misbehavior can be punished in the case of future activity in the ledger. Restricted distributed ledgers also expose the conduct of any participants in the DLT network to the set of rules and law-enforcement measures that typically apply to off-ledger activity.

Available at: <https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf>

⁶⁸ *Id.*, at 14.

A second type of validation system is a proof-of-stake (PoS) consensus process. This assigns shares of validation rights to users according to their stake in the system. How a validator’s stake is to be measured is thus a critical aspect of a system of this type, and different DLTs take different approaches. Some possible criteria used to measure a validator’s stake are the amount of tokens owned, the amount of particular native tokens or off-ledger assets escrowed in the ledger as collateral, or the reputation of the validator in a restricted DLT (known as “proof-of-identity”).

⁶⁹ *Id.*, at 14.

⁷⁰ Intel created two new consensus protocols: “Proof-of-Elapsed-Time” (PoET) and Quorum Voting (QV). Both are available in Sawtooth Lake. PoET is a lottery protocol that builds on Trusted Execution Environments (TEEs) provided by Intel’s Software Guard Extensions (SGX) as a way of dealing with a large population of participants. QV is an adaptation of the Ripple and Stellar consensus protocols and serves to address the needs of applications that require immediate transaction finality. On Ripple see: David Schwartz, Noah Youngs & Arthur Britto, *The Ripple Protocol Consensus Algorithm*, available at: https://ripple.com/files/ripple_consensus_whitepaper.pdf The Ripple consensus algorithm circumvents the requirement that all nodes within the network communicate synchronously. It utilizes collectively-trusted sub-networks within the larger network. On Stellar see: David Mazières, *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*, STELLAR DEVELOPMENT FOUNDATION, available at: <https://www.stellar.org/papers/stellar-consensus-protocol.pdf> The Stellar consensus achieves robustness through quorum slices – individual trust decisions made by each node that together determine system-level quorums. Slices bind the system together. Compared to decentralized proof-of-work and proof-of-stake schemes SCP has modest computing and financial requirements.

For Sawtooth Lake Intel developed two new consensus protocols: “Proof-of-Elapsed-Time” (PoET) and Quorum Voting (QV). Both are available in Sawtooth Lake. PoET is a lottery protocol that builds on the Trusted Execution Environments (TEEs) provided by Intel’s Software Guard Extensions (SGX). PoET helps Sawtooth Lake deal with a large population of participants. QV in contrast, is an adaptation of the Ripple and Stellar consensus protocols. QV allows Sawtooth Lake to address the needs of applications that require immediate transaction finality.

PUTTING INTRA-COMMUNITY EU VAT TRANSACTIONS ON THE BLOCKCHAIN

As of the second quarter of 2016 a significant number of advances have been made in permissive distributed ledger technology. Major technology companies are now on board contributing to design and workability.⁷¹

Leading global companies, from IBM, Intel, and Microsoft to Nasdaq and DNB [Dutch Central Bank], are adopting new plans to benefit from the blockchain technology through streamlining their processes. They are seeking to upgrade the common state of their business and gain an edge against rivals.⁷²

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 earlier, under current law for 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.⁷³ Similar rules apply in cross-border B2B sales of services.⁷⁴

⁷¹ Microsoft provides a Blockchain-as-a-Service (BaaS) platform through Azure. It promises “... an open, flexible, and scalable platform supporting a growing number of distributed ledger technologies that are designed to address specific business and technical requirements for security, performance, and operational processes.” <https://azure.microsoft.com/en-us/solutions/blockchain/>. For example, Kyt Dotson, *Storj beta Added to Azure BaaS Ecosystem, ShapeShift hacked, Kraken Series B investment* BITCOIN WEEKLY (April 13, 2016) available at: <http://siliconangle.com/blog/2016/04/13/bitcoin-weekly-2016-april-13-storj-beta-added-to-azure-baaS-ecosystem-shapeshift-hacked-kraken-series-b-investment/> (discussing the Storj Labs Inc., a developer of blockchain-based end-to-end distributed and encrypted cloud-based storage service, announcement that as of April 9, 2016 a beta version of its blockchain product on Azure BaaS where it will bring its product to enterprise-level users as an API that is accessible through Azure BaaS).

⁷² Olusegun Ogundeji, *From Microsoft to Nasdaq: Blockchain Is Gaining Unprecedented Traction*, THE COINTELEGRAPH, (April 21, 2016) available at: <http://cointelegraph.com/news/from-microsoft-to-nasdaq-blockchain-is-gaining-unprecedented-traction>

⁷³ Supra note 37.

⁷⁴ The taxation of services, particularly intangible services have proven problematical for the EU. When the Commission submitted its proposal for the Sixth Directive cross-border supplies of *intangible services* (Art. 56(1)(a) to (f) RVD, formerly Art. 9(2)(e)) were exempt (in the jurisdiction of the supplier) and were subject to a reverse charge (in the jurisdiction of the business buyer). This treatment matched the post-1991 treatment for the cross-border supply of goods. However, when the Sixth Directive was adopted a different approach was used (to chieve the same end) – a deeming provision changed the place of supply from the seller to the buyer’s jurisdiction. In Amendments of October 11, 1974 the Commission added paragraph 3 to proposed Article 10:

For the purposes of charging tax on supplies referred to in Article 2(3) the place where the service is received shall be deemed to be the place where the business of the person receiving the service is established or, in the absence of such place, the place where he has his permanent address.

Both the seller's jurisdiction (which will be required to issue a VAT refund to taxpayers making these cross-border supplies) and the buyer's jurisdiction (which will be waiting for VAT to be remitted when these cross-border acquisitions are consummated) have an interest in confirming the legitimacy of the transaction.

The full commercial chain will be more complex, but that does not concern us here. There will most likely be B2B transaction preceding the seller's cross-border supply, and most likely further B2B (or B2C) transactions following the buyer's acquisition. These additional transactions will be included when a full application of *distributed ledger technology* to VAT compliance is considered. These are domestic areas are concerned with different frauds. They cannot be examined here. Follow-up articles will consider these points.

Example

Assume an automobile manufacturer in France produces 100 cars for export that are sold to "Seller A" for €10,000 euro each (a domestic sale). "Seller A" reaches agreement with "Buyer B" in the Netherlands to acquire 10 of these cars for €11,000 each (an intra-community cross-border sale). After import "Buyer B" re-sells the cars to a Dealer in the Netherlands who sells on to individual Dutch final consumers.

Assume that a distributed VAT ledger records the transactions involving each of the 10 cars from the manufacturer acquisition of materials to produce the 10 cars (Block 1), which are transferred to Seller A (Block 2).⁷⁵ The stage we are concerned with is the cross-border sale to Buyer B in the Netherlands (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 in the distributed VAT ledger.

When Seller A and Buyer B agree to the terms of the sale/ purchase of the 10 autos for €11,000 each, the rules of the distributed VAT ledger will require both parties to transmit this tentative agreement (a *pro forma* invoice) in an encrypted xml file to their respective tax administrations. From there it will pass to the cloud, and then to each of the assigned nodes in each jurisdiction.

In this example, because Eurostat records the French GDP (2015) at €2,183.6 billion, and the Dutch GDP (2015) at €678.5 billion, France will be required to dedicate 21 nodes to this

Article 196 RVD [formerly 21(1)(b)] then required that a reverse charge be applied when these services were rendered by a taxable person established in the Community to a taxable person in another Member State or by a taxable person established outside the Community.

⁷⁵ A blockchain is simply a chronological database of transactions recorded by a network of computers. Each block is encrypted and organized into smaller datasets referred to as "blocks." Every block contains information about a certain number of transactions, a reference to the preceding block in the blockchain, as well as a consensus notation indicating that the current block has been validated. Thus, each block contains the hash of the previous block, which thereby fixes the current block as the sole antecedent. All operations in the blockchain are validated through a digital fingerprint created through a particular hash function (SHA256 is used by Bitcoin). All transactions incorporated in the blockchain are mapped into a fixed-length string of data. Any differences in input data will produce differences in output data (and thus a different digital fingerprint). See: Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, at 6-7, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

exercise, and the Netherlands will be required to provide 6. With the assistance of artificial intelligence (AI) each of the nodes will be asked to approve or disapprove the proposed transaction.⁷⁶ If we further assume that the consensus threshold is set at 75% of the French nodes and 75% of the Dutch nodes, then consensus would be registered (automatically) if approvals at this level were reached.

The invoice is the most critical VAT document. A uniform law change will be required throughout the EU. It will require that every valid VAT invoice must display a digital fingerprint derived through the VAT blockchain consensus process. The fingerprint will identify that Block 3 is permanently linked to Block 2. The entire history of the commercial chain can be followed in this manner. 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.

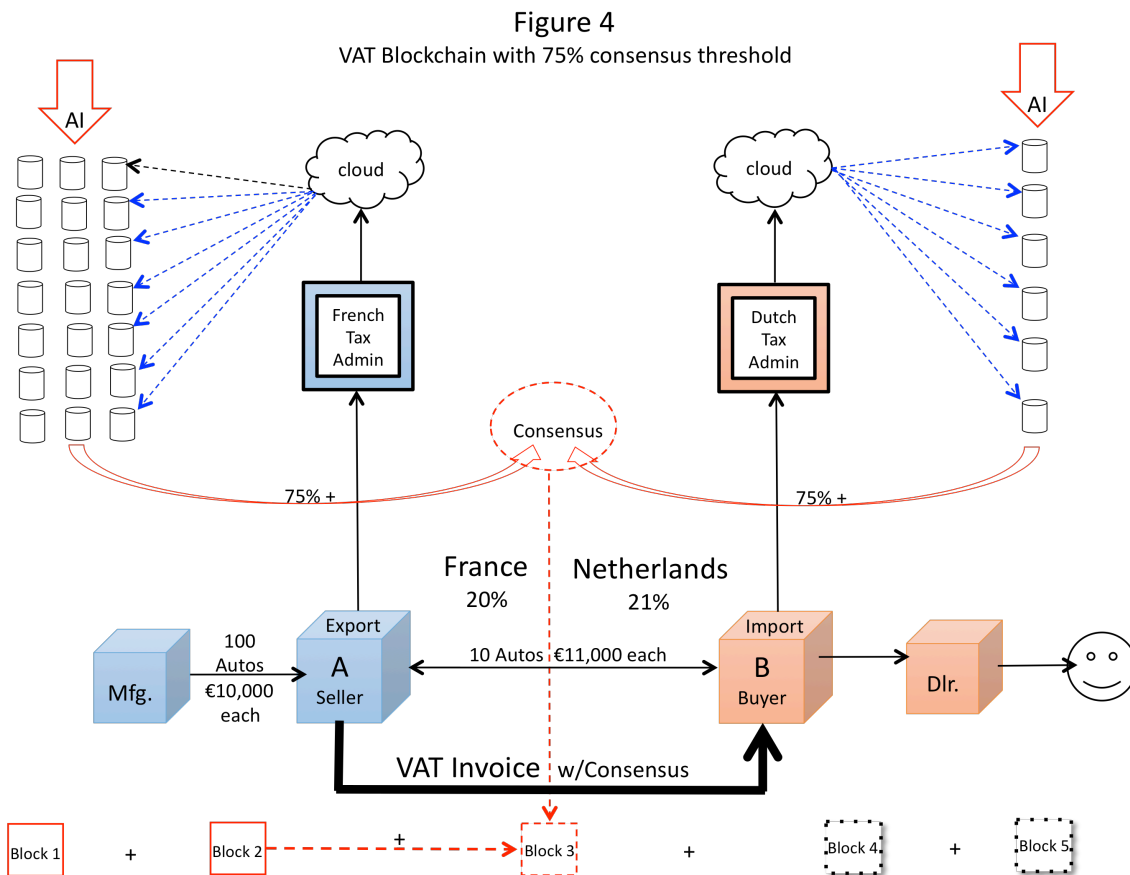
To perform its function each node will need to have immediate access to all standard invoice-level data about both parties (name, address, VAT ID, price of each item, volumes involved). In addition, all nodes will be able to conduct AI-facilitated risk analysis. Because they are government-nodes, each will have access to large number public and private databases (in the same manner as an auditor would). Statistical anomalies will be identified in real-time, and authorities will be alerted. AI will move (or be directed) through available data points. Analytical approaches preferred by node managers will guide the analysis. For example, points of inquiry would include:⁷⁷

- Are the prices charged below market?
- Is the buyer or seller a newly registered taxpayer with insufficient capital to engage in transactions like those proposed?
- Has either tax authority specifically notified one party that previous deals involving the supplier had been traced to a VAT loss and/or had involved carousel movements of goods?
- Has either tax authority specifically notified one of the parties to the current transaction that other MTIC VAT fraud characteristics (such as third party payments) have occurred in other transaction chains by this taxpayer?
- Are the buyer and seller current on other tax obligations (income tax, property taxes, payroll taxes)?
- Based on available payroll records do the buyer and seller appear to have a sufficient number of employees to justify the transaction volumes on the proposed invoices?
- What is the buyer's/supplier's history in the trade?
- Does the deal carry no commercial risk – e.g., no requirement to pay for goods until payment received from customer?
- Does the deal involve consistent or pre-determined profit margins, irrespective of the date, quantities or specifications of the specified goods traded?

⁷⁶ SmartCloud Inc. performs risk analysis for 60,000 taxpayers handling 2 million transactions per day. AI of this quality installed at each node could more than handle the commercial transactions on a DICE blockchain. Personal communication, Paul Lindenfelzer, Partner, VP Sales and Operations, SmartCloud, Inc., (Bedford, MA) July 11, 2016 (plindenfelzer@smartcloudinc.com).

⁷⁷ For other examples see the due diligence requirements listed at: HM Revenue and Customs, *VAT Notice 726: joint and several liability for unpaid VAT* available at: <https://www.gov.uk/government/publications/vat-notice-726-joint-and-several-liability-for-unpaid-vat/vat-notice-726-joint-and-several-liability-for-unpaid-vat>

- Does the supplier (or another business in the transaction chain) require 3rd party payments or payments to an offshore bank account?
- Are the goods adequately insured?
- Are goods of high value offered with no formal contractual arrangements?
- Are high value deals offered by a newly established supplier with minimal trading history, low credit rating etc?
- Can a brand new business obtain specified goods cheaper than a long established one?
- Does the volume purchased (or sold) fit within normal trading patterns for these companies?



CONCLUSION

Increased fraud detection. As with the original DICE proposal, putting invoice data into a blockchain will not eliminate the *first instance* of MTIC/ MTEC in a fraud chain, but it should detect (in real-time) any subsequent efforts to continue the fraud. The *first transaction* in a fraud chain (that is, the first trade by a soon-to-be missing trader) may nevertheless be detected if, for

example, the commercial volumes by a new trader are too exceptionally high for the marketplace. But this is not assured.

Improved domestic enforcement. If adopted, a blockchained DICE system would inevitably alter how tax authorities would approach the detection of MTIC/ MTEC fraud. A blockchained DICE regime would prompt intensive domestic data gathering, frequent record updating, and frequent accuracy checks of local taxpayers. This would be a dramatic change from the current efforts. Audit and investigation are retrospective currently, and can result in massive global searches for largely foreign fraudsters who had set up shell companies to carry out local frauds and then gone into hiding overseas.

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

Increased audit efficiency. All tax administrations have limited audit resources, and current efforts to stop MTIC/ MTEC frauds are consuming huge amounts of time and effort. For a good example, we need to look no further than the current German enforcement action into the huge CO2 MTIC fraud that arose in late 2009 and early 2010. Deutsche Bank enabled this fraud, and it had a huge revenue impact in two countries. Staggering numbers of CO2 permits were sold back and forth between the Frankfurt head office and the London branch of Deutsche Bank.⁷⁸ The permits were funneled into Deutsche Bank from newly established German and UK companies. These “feeder” companies were for the most part established by foreigners, which sent the German tax authorities overseas to find suspects.⁷⁹

The tentacles of the Deutsche Bank fraud spread throughout Germany and the UK. The permits went in a complete circle (a true carousel fraud). Prior to an August 1, 2009 law change in the UK (which zero-rated CO2 permits) it was the UK revenue that incurred substantial losses.⁸⁰ German revenue losses mirrored those in the UK, but after August 1, 2009 they accelerated⁸¹ well beyond what the UK had experienced. The fraud was over quickly. But, it

⁷⁸ Richard T. Ainsworth, *VAT Fraud Mutation, Part 3: “Pull” Missing Trader Fraud and Deutsche Bank*, 81 TAX NOTES INTERNATIONAL 3706 (March 28, 2016).

⁷⁹ See for example the extradition hearings of Samir Azizi (*In the Matter of: the Extradition of Samir Azizi, Order Granting Motion for Certificate of Extraditability* 5:14-xr-90282-PSG (March 20, 2015) District Court, N. D. CA.) and Mohammad Safddar Gohir (*Complaint for Provisional Arrest with a View Towards Extradition, United States v. Mohammad Safddar Gohir*, Docket No. 2:14-mj-314-CWH (D. NV filed May 4, 2014). Arrest warrants were also issued for Faisal Zahoor Ahmad (British national); Rakesh Sharma (British national); Muhammad Ashraf (Pakistani national) Mobeen Iqbal (Pakistani national); Iftakhar Ali (British national); Arfan Khan (British national); Franz Mir (British national); Mohsin Salya (British national).

⁸⁰ Deutsche Bank claimed refunds attributable to CO2 from the UK of £15.14 million and £48.14 million in June and September of 2009. *Id.*, at 1140.

⁸¹ Deutsche Bank claimed VAT refunds of €220 million attributable to CO2 from Germany. *Id.*, at 1139. But, in addition, Deutsche Bank had already conceded in 2011 that a correction was needed on its CO2 claims in 2009 of €150 million. This was in the summer of 2011. By the end of 2011 Deutsche Bank indicated that an additional

took an April 2010 raid of the Deutsche Bank head office in Frankfurt (and other locations throughout Europe) by 500 police officers to bring it to a close.⁸²

Beyond the EU. The beauty of blockchain is that it is *trustless*. Participants do not have to trust each other to use it with confidence. Imagine a data exchange between Poland and Russia in an investigation into MTEC frauds. Would either side be inclined to provide timely access to centralized data files on their own taxpayers? If access is granted, would either side trust the accuracy of the data?

With a distributed VAT ledger Russia could join the ledger just as easily as any EU jurisdiction. Trade between Russia and Poland would be treated no differently than trade between Poland and Germany. If consensus was reached on the validity of a block of transactions, the data within the block could be trusted. Blockchain extinguishes the need for a centralized data repository. It is *trustless*.

The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust.⁸³

This is precisely what is needed to combat MTIC/ MTEC frauds.

€160 million correction was needed on its 2009 CO2 permit reclaims. Roughly, €530 million was inappropriately claims by Deutsche Bank. *German Bank CEO Fitschen complains (by) phone – The Co-head of Deutsche Bank complained with a phone call to Prime Minister of Hess Bouffier on tax raid*, ZEITONLINE (December 16, 2012) available at: <http://www.zeit.de/wirtschaft/unternehmen/2012-12/deutsche-bank-fitschen-bouffier-hessen-anruf>

⁸² Matthew Carr & Karin Matussek, *Deutsche Bank, RWE Raided in German Probe of CO2 Tax (Update 2)* BLOOMBERG (April 29, 2010) available at:

<http://www.bloomberg.com/apps/news?pid=20601130&sid=aIPHf4UHkqU>

⁸³ THE ECONOMIST, *The Promise of Blockchain: The Trust Machine* (October 31, 2015) available at:

<http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>.