A hybrid blockchain proposal to improve value added tax recovery

Christophe Gaie*

Direction Interministérielle du Numérique,
20 Avenue de Ségur, 75007 Paris, France
Email: christophe.gaie@gmail.com
*Corresponding author

Markus Mueck

Intel Deutschland GmbH,
85579 Neubiberg, Germany
Email: Markus.Dominik.Mueck@intel.com

Abstract: In the present article, the authors propose a novel hybrid blockchain approach to improve VAT recovery, meeting privacy requirements as introduced by the European General Data Protection Regulation. This will provide real improvement to prevent tax fraud as it will not be possible to hide cash transactions. To limit the amount of energy spent, the idea proposed in this paper is to introduce an authority with a limited action. Moreover, the authors address privacy requirements by providing two cumulative possibilities: (1) separate privacy related and other information; and (2) introduce blockchains pointers to ensure the integrity of the blockchain. Lastly, the paper underlines how government administrations are able to take advantage of the proposed new approach to struggle against illicit transactions.

Keywords: data analytics; fraud detection; tax recovery; telecommunications; blockchain; privacy protection.

Reference to this paper should be made as follows: Gaie, C. and Mueck, M. (2022) ‘A hybrid blockchain proposal to improve value added tax recovery’, *Int. J. Internet Technology and Secured Transactions*, Vol. 12, No. 1, pp.27–37.

Biographical notes: Christophe Gaie is currently working for the French Prime Minister Services. He is in charge of the inter-administration exchange platform and ensures the functioning of multiple APIs. Formerly, he was the IT team leader in charge of the computation of the income tax and the tax property wealth for the French Tax Administration. He was deeply involved in the establishment of withholding tax on personal revenues. In 2010, he received his PhD in Telecommunications from the University of Paris Saclay-Supelec. His main areas of interest are computer science, IT modernisation, API management, data flow and artificial intelligence.

Markus Mueck received his Electrical Engineering Diploma degrees of University of Stuttgart, Germany and Ecole Nationale Supériere des Télécommunications (ENST), Paris, France in 1999 and the doctorate degree of ENST, Paris, France in 2006. He is a Senior Standardisation Manager at Intel Mobile Communications, Germany, Adjunct Professor at University of Technology, Sydney, Australia, Vice-Chairman of the Board at ETSI, Chairman of ETSI Reconfigurable Radio Systems Technical Body, Chairman of 5GAA WG on Standardisation and Chairman of the IEEE Special Interest Group on Cognitive Radio in 5G.

1 Introduction

What is a blockchain? Basically it is a decentralised architecture which enables secure information sharing among multiple nodes in a distributed network. The blockchain relies on the cooperation of nodes which ensures the reliability of the information by 'mining' new blocks and performing 'proofs of work'. The most famous blockchain is the Bitcoin created in 2009 by Nakamoto.

The Bitcoin is considered to be a cryptocurrency which can enable peer-to-peer legal or illegal transactions. Although the Bitcoin has proven its reliability and its interest for users, gaithe Bitcoin has certain disadvantages for governmental organisations.

The main disadvantages of Bitcoin are described below:

- The mining requires a substantial amount of electrical power which is not suitable in a context of global warming.
- The relative secrecy of transactions as the only information shared is the IP address. This can simplify illegal transactions as well as laundering since cryptocurrencies can be retained in tax heavens.

In this paper, we aim to take advantage of the blockchain architecture to ensure immediate VAT recording. We propose a novel approach comprising the following features:

- We introduce a hierarchical blockchain architecture which enables the removal of information as it may be required due to privacy requirements as given by the European General Data Protection Regulation (EU, 2016); for the same purpose, we furthermore outline that a blockchain may contain pointer to information instead of the actual.
- A separation of privacy related and other information allows to keep non-sensitive information within the blockchain and thus its integrity is ensured at any time.
- We propose to introduce an authority in order to reduce the power consumption, ensure identification of every actor implied in transactions and enable VAT compensation computation.

With the upper approach, it is outlined how efficient blockchain-based VAT management can be achieved, meeting privacy requirements and enabling for dynamic modification of the information. At the same time, Government agencies will be able to use the blockchain in order to identify illicit and suspicious transactions.

In state of the art literature, Okazaki (2018) advocates that the blockchain transparency makes fraud and errors far easier to detect. However, the author underlines that this advantage may not apply in reality as it requires that the tax authority disposes of every transactions even the handmade transactions. This barrier may be removed, by restricting cash usage and ensuring that cash registers keep an electronic track of every transaction.

Fatz et al. (2019) also propose to improve tax compliance by introducing a blockchain technology in business processes. Indeed, they we provide a conceptual design and a prototype for compliant process execution in the context of value-added taxes. The authors underline two challenges in this context. First of all, they have to ensure privacy of information. Secondly, the blockchain architecture does not solve the potential breaches of information existing in the source IT system.

Okazaki et al. (2019) propose a blockchain-based solution which ensures data confidentiality in the context of invoice financing. The blockchain architecture proposed benefits from transparency, immutability, trustworthiness, and security. It also provides a reputation evaluation of entities offering the ability to modulate the cost of the insurance. The proposal relies on Ethereum smart contracts (see Wood, 2017). The confidentiality relies on the encryption of data and computation of a hash stored in the Ethereum blockchain.

Another approach was described by Hyvärinen et al. (2017), indeed propose a blockchain-based prototype system aimed at eliminating tax fraud in the context international exchange. The proposal is based on the specific context of the Danish tax authority with potential applications to track international fraud. The authors underline that blockchain provides a comprehensive solution (including infrastructure, application and presentation levels) that can be implemented by every actor. However, the proposed blockchain-based solution presents some limitations in terms of scalability, privacy and cost efficiency.

In 2018, Risius and Spohrer describe the different perspectives of blockchain research and insist on the limits of previous research, focused on technological questions of design and features. They advocate on the huge perspectives of blockchain research which can address different activities (design and features, measurement and value, management and organisation) and levels of analysis (users and society, intermediaries, platforms, firms and industry). Moreover, the authors detail multidisciplinary research approaches (computer science, information systems, law, finance, political science…) and we advocate to extend it to tax recovery.

Then, Truby (2018) underlines that the Bitcoin implementation of blockchain technology has environmental drawbacks. Indeed, the transaction verification process is heavy and consumes a large amount of energy. The author provides a large review which tackles the problem of sustainability and provides an analysis of potential fiscal policy to promote green blockchain. In the present paper we propose a hybrid architecture which takes into account the climate objective by leaning on a central authority.

Moreover, Ainsworth and Alwohaibi (2017) underline the interest of introducing a blockchain to improve tax compliance, especially for inter-country exchange. They insist on the advantages of this distributive technology compared to centralised ones and propose to apply it to Gulf countries where VAT is being introduced. This situation is well suited to experimentation as it is easier to add a new functionality to a new system that modifies an existing one (this is a ‘leap-frog effect’). This paper is introducing interesting concepts, but it does not tackle the problem of power consumption of such a system and the specificity of intra-country VAT exchange.

We furthermore exploit recent advances of the European Telecommunications Standards Institute (ETSI). ETSI is currently developing two specifications (ETSI GR PDL 001, in press; ETSI GR PDL 003, in press) which discuss a generalised approach, building on the theory of distributed ledgers. A distributed ledger is indeed a type of database spread across multiple sites, regions, or participants. Blockchain is one type of distributed ledger. While blockchains consist of a sequence of blocks, distributed ledgers do not necessarily require such a chain. Furthermore, distributed ledgers do not generally need proof-of-work which is an advantage for scaling.

Finally, we outline the importance of strengthening the blockchain integrity as there exists a large scope of possible attacks. Indeed, Zhang and Lee (2020a, 2020b) described multiple attack scenarios which rely either on diverting the blockchain processes: majority consensus; proof-of-work; proof-of-stake… Their research is carried out in the context of fifth-generation (5G) network era where blockchain-based mobile-edge computing plays an important role. To mitigate these risks, the authors proposed a new efficient a group signature scheme to BMEC to verify blocks efficiently. They proposed optimisation strategies to struggle against double-spending with Sybil attacks and provided measures to mitigate which rely on introducing an identity fee and setting a deadline to defend against the attack.

The remainder of the paper is organised as follows. Section 2 introduces a hybrid blockchain model enabling VAT recovery. Section 3 further introduces solutions for meeting privacy requirements, followed by Section 4 where it is explained how to proposed scheme is used for the identification of illicit or suspicious transactions by government agencies. Section 5 finally gives the conclusions.

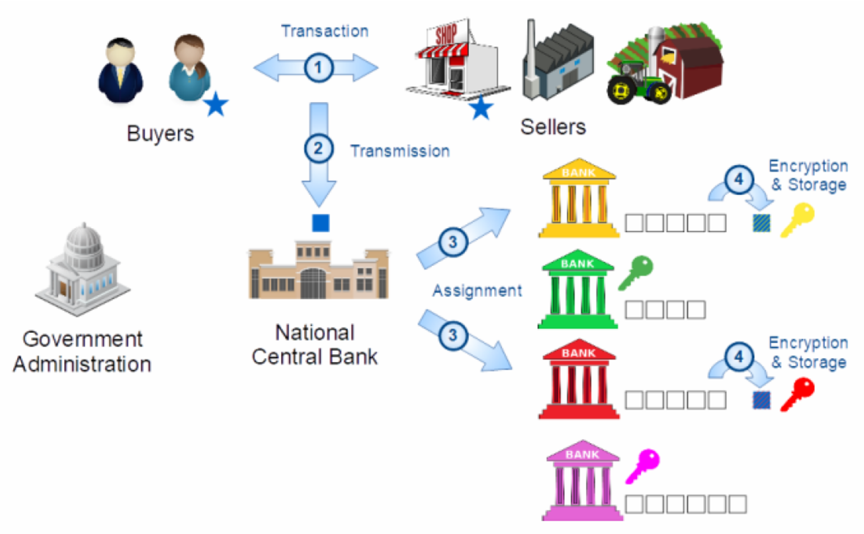
2 Hybrid blockchain architecture for VAT recovery improvement

In this section we propose a new architecture to improve VAT recovery. The idea is to take advantage of the decentralised blockchain architecture while introducing an authority which enables to reduce power consumption for an equivalent transaction security. This architecture does not take into account international exchanges which will be addressed in a future paper.

The basic idea described in Figure 1 is to generate a block identifying each transaction and store it securely. This block should contain information: identification of the buyer, identification of the seller, amount of transaction without tax, VAT collected, date of transaction, etc. Step 1 consists in identifying the transaction between a buyer and a seller and generates a transaction block. The thrust of this proposal is to link cash flows and accounting. The NCB plays a central role as it ensures that each data transfer is tracked by multiple separate banking institutions.

Then, the block should be transmitted to the National Central Bank (for instance, the French NCB is Banque de France, the German NCB is the Deustche Bundesbank, the Spanish NCB is the Banco de España, and so on). Step 2 enables to ensure the system transparency and coordination. Moreover, as the National Central Bank is an independent authority, this ensures the recovery securisation. In this paper, the authors do not tackle directly the financial transaction itself but the funds could be directly separated (the pre-tax amount from the buyer to the seller and the tax amount from the buyer to the NCB). This would ensure that the seller would never be able to retain VAT, which is a well-known problem of VAT recovery [see Smith and Keen (2007) for chain evasion or carousel fraud explanations].

Figure 1 Hybrid blockchain architecture proposed (1/2) (see online version for colours)



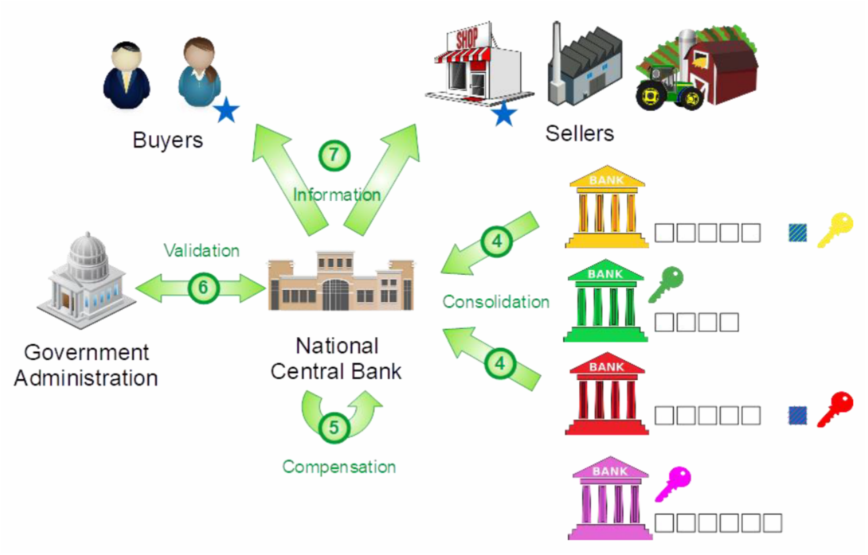
Step 3 consists for the NCB to assign blocks to at least two different banks from the national system without any financial link. This assignment aims to record every transaction and be able to prove any transaction at any moment. In contrast to usual blockchains where every actor possesses a copy of the whole blockchain, the authors underline that economic information are private and should only be known by the involved actors, their banks, the NCB and the fiscal administration. To preserve the decentralised architecture, the authors propose to delegate shelf registration to specific trusted third-parties (which have to be independent from the two initial banks).

Therefore, we propose that each bank possesses its own blockchain which is also shared with the NCB, but only for dispute resolution. Only authorised actors may access to this information which is still decentralised in its normal usage. The information storage is performed in step 4.

Furthermore, we introduce a separation of highly sensitive privacy related and other information. The latter can be contained in the blockchain itself while it may be preferable to rather include pointer to sensitive private information, possibly stored in independent blockchains in order to preserve the overall integrity. Section 3 will further discuss related solutions.

The idea described in Figure 2 is to rely on the hybrid blockchain architecture proposed to perform VAT compensation and recovery. Indeed, a seller does not necessarily transfer the whole VAT recovered to the fiscal administration. The amount of VAT to give back is reduced by the VAT already paid to intermediate firms (when the seller was itself a buyer). The interest of building a reactive blockchain is to identify at every moment the amount of VAT paid or due by each actor of the economy and recover VAT more easily.

Figure 2 Hybrid blockchain architecture proposed (2/2) (see online version for colours)



Step 4 ensures the periodic consolidation of transactions retained in each bank. As the National Central Bank keeps a copy of every bank blockchain, the consolidation aims to verify the conformity of information using HMAC (keyed-hash message authentication code) involving a cryptographic hash function and a secret cryptographic key. This process should be performed every week or every month depending on the national legislation. The weekly choice provides better reactivity but reveals more stringent for banks and actors.

Step 5 aims to compensate the different VAT payments between actors. This functioning is different from the usual process where each VAT debt or credit is due or claimed directly to the fiscal administration. The introduction of a compensation process does not simplify the computation process as it is required to keep track of all compensations to ensure account liability. However, the amount of transactions is highly reduced as the NCB will firstly transfer funds to the fiscal administration and then give back funds to firms (at most one transfer to the bank holding the firm accounts). It is important to underline that this new process would be a huge change in the national law and for many fiscal administrations. To ensure the completeness of the system, the authors propose that cash registers generate a dematerialised flow of information.

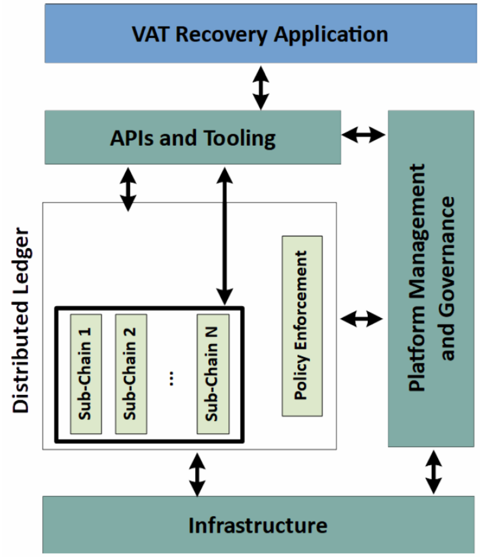
Step 6 is an exchange between the NCB and the fiscal administration. Indeed, the VAT process should be verified periodically and the fiscal administration could reject some VAT credit or freeze it until validation. Therefore, the compensation described in the previous step can be slightly modified before the funds are transferred to the different actors. This could avoid some massive fraud by taking advantage of the experience of tax verification professionals (and/or fraud detection systems which can be based on artificial intelligence).

Step 7 is the information exchange of each actor in parallel to the transfer of funds. The information is transmitted to banks but also to involved actors. The bill can be sent simply by mail but the authors propose to use a secured portal (provided by the NCB or the fiscal administration) where the actor may connect and get every useful information.

3 Further generalisation and consideration of privacy requirements

Following the basic concepts above, we propose a further generalisation of the blockchain architecture for VAT recovery. In particular, we suggest that the distributed database approach relying on a blockchain may be complemented by further distributed ledger type of sub-chains are illustrated in Figure 3 and based on ETSI's proposals (ETSI GR PDL 003, in press):

Figure 3 Generalisation of the blockchain architecture to multiple distributed ledgers (see online version for colours)



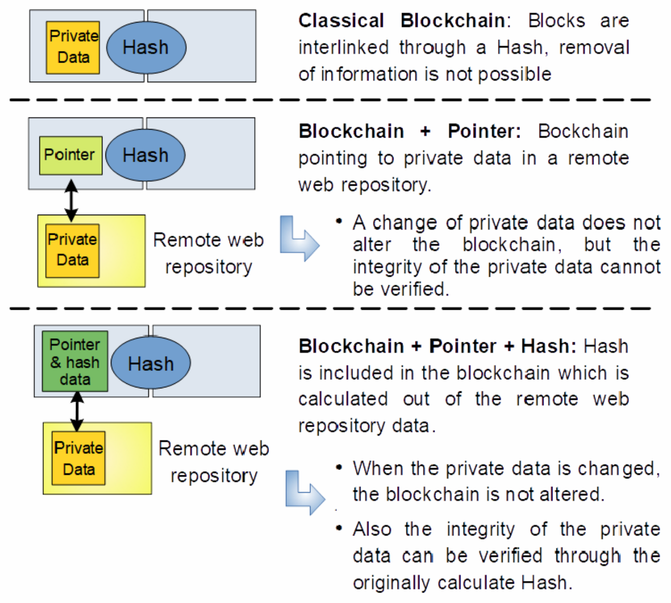
Note: The sub-chains should be connected to the infrastructure.

We furthermore consider that highly sensitive privacy related and other information are separated; some (or all) of the sub-chains indicated above may comprise personal data which are potentially protected under the European General Data Protection Regulation (EU, 2016).

This is a major challenge for blockchain type of approaches, since the owner of the data is granted a number of rights, including the right to request the removal of its information from a related database and thus from the blockchain. A blockchain, on the other hand is exactly designed in such a way that the integrity of the data is always guaranteed and thus a removal of information elements would require a re-creation of the entire blockchain from the beginning. A separation of privacy related and other data simplifies the overall data management approach.

A known approach for mitigating this issue is indicated in ETSI GR PDL 003 (in press). Indeed, it is suggested not to include the actual data itself which may fall under the GDPR, but rather a pointer to the data, for example on a (protected) website. This solution is illustrated in line B of Figure 4. It has the disadvantage that we cannot be certain about the integrity of the data on the target storage site.

Figure 4 Illustration on management of remotely stored private data through a pointer in combination with a hash (see online version for colours)


Private Data
Hash
Classical Blockchain: Blocks are interlinked through a Hash, removal of information is not possible
Pointer
Hash
Private Data
Remote web repository
Blockchain + Pointer: Bockchain pointing to private data in a remote web repository.
• A change of private data does not alter the blockchain, but the integrity of the private data cannot be verified.
Pointer & hash data
Hash
Private Data
Remote web repository
Blockchain + Pointer + Hash: Hash is included in the blockchain which is calculated out of the remote web repository data.
• When the private data is changed, the blockchain is not altered.
• Also the integrity of the private data can be verified through the originally calculate Hash.

We propose therefore a novel element in the proposed solution: We propose that a Hash is created [typically building on the Hash Algorithm used for the blockchain such as SHA256 for example (US Department of Commerce et al., 2015)] based on the information of the target website. This Hash is proposed to be included together with the pointer to the targeted web repository into the concerned block of the blockchain, as illustrated online C of Figure 4.

In this way, the information stored at the target web repository can be altered, but in this case the integrity of the site is lost because the Hash is altered. The remote web repository is thus invalidated and no longer used. This can be verified through a recalculation of the hash based on the available data on the web repository. At the same time, the content of the blockchain remains unchanged although the private data of a user has been removed. Indeed, the blockchain only depends on the pointer value but not on the data itself.

The reader should notice that, as described by Gürcan et al. (2018) enabling the cancellation of transactions in a blockchains increases its fairness and consequently its security.

The principles described in the current paper are illustrated in Figure 4 and classified by increasing data security.

It is important to notice that the remote web repository should be secured and different from the common web repository. The repository should be designed as a bank’s safe-deposit box (only the owner or strongly authorised agents can access to this secured information).

Thus, we recommend to apply the following security protection measures to this specific repository:

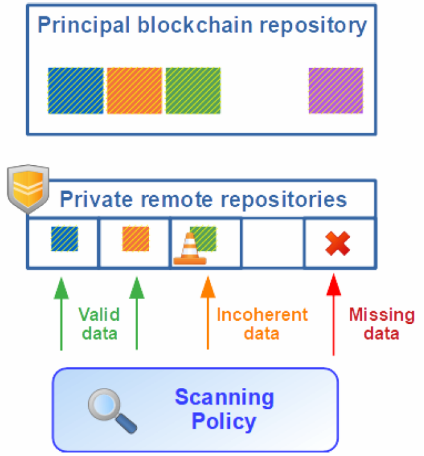
- a higher security level as it will host private data
- a control of access to identify and keep a track of each person who consults this information
- a relative proximity with the associated blockchain (in the same IT centre) as it can be required to read this data periodically
- a specific redundancy which enables to restore data when a failure appears or an attack is detected.

4 Scanning the blockchain to detect suspicious transactions

An interesting approach consists in scanning privacy data in order to detect suspicious transactions. Different kind of information can be obtained through scanning:

- *validation* which means that data do not present any detectable abnormality
- *incoherent or suspicious* which means that this data has to be verified by a specialist or a specific fraud detection algorithm
- *missing* which means that the data cannot be found and that the transaction has to be verified.

Figure 5 Scanning policy for fraud detection (see online version for colours)



In order to facilitate the implementation of the proposed architecture, we also define some key concepts for the scanning policy:

- *Adjusted periodicity* which means that the entity in charge of fraud detection has to define the appropriate scanning periodicity. Intuitively, this should at least be a monthly period to fit with the VAT recovery process.
- *Unique global verification* which means that a data should be checked only once to limit the scanning effort. However there may be some exceptions in case of

dedicated or specific controls (targeting a particular transaction or a new type of fraud).

- *Permanent scanning adjustment* which means that the scanning tool should include regularly new detection policies. As fraud schemes are continuously evolving the fraud detection policies should respect the same principle.

As indicated by Hao et al. (2014), the readers should notice that scanning tools were developed in the context of end-to-end verifiable voting protocols such as Adder, Civitas, Helios, Scantegrity… These solutions are similar to the current situation. They involve three actors which could be adjusted to the VAT context as follows:

- ordinary voter may be replaced by the association Buyer-Seller involved in a transaction
- auditor may be compared to the banks which verify the transaction before recording it
- universal verifier may consist in the NCB or a third-party with the control delegation granted by NCB.

5 Conclusions

In the present paper, a novel blockchain approach was presented enabling an efficient VAT recovery. The proposed scheme considers a number of requirements including privacy protection [as required by GDPR (EU, 2016) in Europe, similar regulatory frameworks exist in other regions] while ensuring the blockchain resilience (removing or altering a piece of information does not compromise the whole the blockchain). A key concept relates to the usage of pointers in the blockchain instead of the actual information. Thus, the information at the target location can be altered or removed without changing the content of the blockchain; therefore the integrity of the blockchain is maintained at all times.

Finally, it is outlined how Government administrations can use the results in order to identify illicit or suspicious transactions and thus to support law enforcement.

References

Ainsworth, R.T. and Alwohaibi, M. (2017) *Blockchain, Bitcoin, and VAT in the GCC: The Missing Trader Example*, Boston Univ. School of Law, Law and Economics Research Paper, No. 17-05, 16 February.

ETSI GR PDL 001 (in press) 'Permissioned distributed ledger', *PDL Landscape of Standards and Technologies*.

ETSI GR PDL 003 (in press) 'Permissioned distributed ledger', *PDL Application Scenarios*.

European Union (EU) (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regards to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)', May, *Official Journal of the European Union*, L 119/1.

Fatz, F., Hake, P. and Fettke, P. (2019) 'Towards tax compliance by design: a decentralized validation of tax processes using blockchain technology', *IEEE 21st Conference on Business Informatics (CBI)*, Vol. 1, pp.559–568

Gürcan, Ö., Pedrosa, A. and Tucci-Piergiovanni, S. (2018) 'On cancellation of transactions in Bitcoin-like blockchains', *26th International Conference on Cooperative Information Systems*, La Valette, Malta, October, (cea-01867357).

Hao, F., Kreeger, M., Randell, B., Clarke, D., Shahandashti, S. and Lee, P. (2014) 'Every vote counts: ensuring integrity in large-scale electronic voting', *The USENIX Journal of Election Technology and Systems*, Vol. 2, pp.1–25.

Hyvärinen, H., Risius, M. and Friis, G. (2017) 'A blockchain-based approach towards overcoming financial fraud in public sector services', *Business & Information Systems Engineering*, Vol. 59, No. 6, pp.441–456.

Nakamoto, S. (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System*, March [online] https://Bitcoin.org/Bitcoin.pdf (accessed 14 October 2020).

Okazaki, Y. (2018) *Unveiling the Potential of Blockchain for Customs*, in WCO Research Paper No. 45, WCO Research Unit, June.

Okazaki, Y., Guerar, M. and Migliardi, M. (2019) 'A fraud-resilient blockchain-based solution for invoice financing', *IEEE Transactions on Engineering Management*, November.

Risius, M. and Spohrer, K. (2018) 'A blockchain research framework – what we (don't) know, where we go from here, and how we will get there', *Business & Information Systems Engineering (BISE)*, Vol. 59, No. 6, pp.385–409.

Smith, S.C. and Keen, M. (2007) *VAT Fraud and Evasion: What Do we Know and What can be Done?*, IMF Working Papers 07/31, International Monetary Fund, March.

Truby, J. (2018) 'Decarbonizing Bitcoin: law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies', *Energy Research & Social Science*, Vol. 44, pp.399–410.

US Department of Commerce, Secure Hash Standard (SHS), Federal Information Processing Standards (FIPS) Publication 180–4 (2015) 31pp., August [online] https://doi.org/10.6028/NIST.FIPS.180-4.

Wood, G. (2017) *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, EIP-150 revision (759dccd–2017-08-07) [online] https://ethereum.github.io/yellowpaper/paper.pdf (accessed 3 January 2018).

Zhang, S. and Lee, J. (2020a) 'A group signature and authentication scheme for blockchain-based mobile-edge computing', in *IEEE Internet of Things Journal*, May, Vol. 7, No. 5, pp.4557–4565, DOI: 10.1109/JIOT.2019.2960027.

Zhang, S. and Lee, J. (2020b) 'Mitigations on Sybil-based double-spend attacks in Bitcoin', in *IEEE Consumer Electronics Magazine*, DOI: 10.1109/MCE.2020.2988031.