Institute for Austrian and International Tax Law Vienna
WU Global Tax Policy Center

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

BLOCKCHAIN 101 FOR GOVERNMENTS

A note prepared for the
FIT International Taxation Conference,
Mumbai, 7-9 December 2018

to equip officials with the essential information about the Blockchain technology and its potential application in public sector domain

Prepared by the WU Global Tax Policy Center (WU GTPC)
at the Institute for Austrian and International Tax Law
of Vienna University of Business and Economics
(WU, *Wirtschaftsuniversität Wien*) and
the Digital Economy Taxation Foundation

Blockchain Overview

The WU Global Tax Policy Center[1] of Vienna University of Business and Economics in collaboration with New Economy Taxation and with support of the Digital Economy Taxation Foundation has embarked on the pioneering research in the field of digital economy and its effect of taxation with respect to compliance and administration. The academic research is enhanced by a series of multi-disciplinary meetings where identified issues are openly and critically discussed between the representatives if academia, government officials and business community. To ensure the global exposure, research is carried out in disperse locations around the world. The following meetings were held successfully: Vienna 15-16 March 2017, Singapore 17-18 August 2017. In 2018 the following sessions will take place: New York 22 May 2018, Singapore July 2018 and China October 2018.

This note is the first output of the Digital Tax Transformation project, which aims to equip the officials with essential information about the Blockchain technology. Application of the blockchain and its underpinning elements: Distributed Ledgers and Smart Contacts with the aim of modernizing and improving public services are at the core of the research.

1. What is blockchain?

Blockchain is a decentralized distributed ledger technology. It allows creation, validation and encrypted transaction of digital assets to happen and get recorded in an incorruptible way.

At its heart, it is a database of groups of transactions (blocks) that are linked to the previous group of transactions (the chain) and is replicated and distributed to everyone who participates in the network so that all copies of the database are identical. Blockchain records every transaction that ever happens, and no records are ever deleted.

[1] https://www.wu.ac.at/taxlaw/institute/gtpc/current-projects/tax-and-technology/

2. What is a distributed ledger?

A distributed ledger is a type of database that is shared, replicated, and synchronized among the members of a network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network.

Participants in the network govern and agree by consensus on the updates to the records in the ledger. No central, third-party mediator, such as a financial institution or clearinghouse, is involved.

Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable history of all transactions in the network.

In short, blockchain can be described as a network of computers, each having an identical copy of the database (distributed) and changing its state (records) by common agreement based on pure mathematics, with no need for any central server or agent to entrust.

3. How is Blockchain Related to Bitcoin?

Bitcoin was the first application of blockchain technology, thus people often inadvertently used "Bitcoin" to mean blockchain. But they are not the same thing.

Bitcoin is a type of unregulated digital currency that was first created by Satoshi Nakamoto in 2008. Also known as a "cryptocurrency," it was launched with the intention to solve the problems of trust, transparency, and accountability between two parties in exchanging money for goods and services over the internet and get rid of third-party payment processing intermediaries.

Bitcoin transactions are stored and transferred using a distributed ledger on a peer-to-peer network that is open, public and anonymous. Blockchain is the underpinning technology that maintains the Bitcoin transaction ledger.

4. Blockchain's Potential Beyond Cryptocurrencies

Bitcoin and other cryptocurrencies relying on blockchain technology may be disruptive but blockchain is of far broader application. While Bitcoin is a crypto-currency ensuring transparency and accountability of financial transactions, blockchain technology can be applied to many other types of transactions to solve the problems inherent in any transaction.

Generally, blockchain technology can be used in a peer-to-peer network of parties, who all participate in a given transaction. The technology uses a distributed ledger that is visible to all parties involved in the transaction. Through a consensus mechanism, the ledger is guaranteed to be consistent. Because the ledger is distributed, everyone involved can see the "world state" at any point in time and can monitor the progress of the transaction.

By its very nature, blockchain is able to tackle the following business issues:

- Trust – Through the use of blockchain, all the parties involved in a transaction only have to trust the blockchain without a need for a central intermediary;

- Transparency – Because the ledger is distributed, all peers involved in the transaction network can view it subject to security rights (see "permissioned" blockchain below);

- Accountability – Since all parties in the transaction can view the distributed ledger, everyone can agree on how the transaction is progressing while it is ongoing, and how it went once it is complete.

The original Bitcoin blockchain implied fully open and permissionless access to the network by any willing party. In this format the main benefit of the nascent technology – decentralization – is realized to the highest degree. Fully open and transparent blockchain-based databases may not, however, be compatible with the requirements and data protection limitations of the public sector. In that case, a permissioned/private or consortium/hybrid type of blockchain may offer a more suitable solution. In the case of restricted access to the blockchain, it is important to achieve the critical mass of the nodes or users on the network not to compromise the essential benefit of the technology, decentralization and to prevent collusion and eliminate the risk of tampering.

See below on differences between blockchain as used in bitcoin and other uses.

5. Why do people predict that Blockchain will change the World?

Beyond cryptocurrencies, the World Economic Forum recently released a report titled The Future of financial infrastructure: An ambitious look at how blockchain can reshape financial services[2] in which it claims that blockchain will play a central role in the global financial system.

(i) Beyond Bitcoin to Transforming Finance

The report revealed that blockchain has the potential to "drive simplicity and efficiency by establishing new financial services infrastructure and processes" and is likely to "form the foundation of next generation financial services infrastructure in conjunction with other existing and emerging technologies." Although the changes in infrastructure won't probably be evident enough to be noticed by consumers, cheaper and faster financial services might become part of the deal if blockchain continues to evolve and eventually becomes "the beating heart" of the finance industry, the report shows. It also estimates that around eighty percent of banks worldwide could start distributed ledger projects by next year and reveals that large central banks are analyzing how this technology will change the way money moves around the globe.

[2] http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

(ii) Beyond Finance

The broader implications of Blockchain beyond finance is described in a recent report by the European Parliament, Blockchain could change the lives of EU citizens[3] with the following potential applications:

(iii) Digital Property Rights

In the area of digital property rights, blockchain technology can assist in identifying copyrighted works and settling disputes. It could lead to multi-territorial licensing policies and improved legal certainty for both creators and purchasers of content.

In the realm of protecting patents, blockchain technology could balance protection of innovators against that of competitors. Blockchain "hashing" and "proof of existence" make the technology helpful in improving the patent system, particularly where there is no unified patent systems across countries. Blockchain technology could make patent systems more efficient and provide more economical proof of existence services.

(iv) Electronic Voting

Blockchain technology can offer a more bottom-up and participatory social structure by providing a cost effective and secure e-voting system.

(v) Smart Contracts

The report noted that smart contracts provide one of blockchain technology's most promising benefits. Smart contracts can improve efficiencies in contract enforcement.

(vi) Supply Chain Management

The report further noted that blockchains are especially helpful for situations where it is important to know ownership histories, such as managing supply

[3]http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA%282017%29581948_EN.pdf

chains. Blockchain technology can improve supply chains by offering infrastructure for certifying, registering and tracking goods and services as they move along the supply chain. Tokens can uniquely identify goods on the blockchain, with each transaction time stamped in a transparent manner.

(vii) Public Administration

The potential "eGovernment" services and applications include identity management, tax collection, land registry, distribution of benefits, digital currencies and any type of government record. Blockchain technology could allow records to be verified and created with greater speed, transparency and security.

(viii) Tax Administration

The blockchain has the potential to disrupt or at least modernize accounting and tax payments. In this context, however, for the benefits of underlying technology to be released, the considerable networking effects are required before it can be implemented. In the long term, blockchain can significantly improve tax compliance by guaranteeing real-time, automated tax payments from the tax payer to the state budget at the time when a transaction in being executed. This is achieved by use of Smart Contracts, pieces of code, programmed to self-execute themselves if and when the set of pre-defined conditions are satisfied. Self-execution allows for unrelated parties to transact with each other in the absence of trusted third party that verifies the validity of transaction. For example, payroll tax can be automatically withheld and paid into the treasury at the time of salary transfer, thus removing the duty of the employer to act as a tax collector. Several benefits are immediately produced: real-time compliance, significant reduction of the transaction costs and elimination of risk of tax evasion and fraud from the outset.

Transparency integral to the blockchain is also arguably capable of providing solutions to beneficial ownership issue[4] in the context of combating illicit tax flaws and prevention of corruption. Opaque corporate vehicles are often exploited by

[4] Julia De Jong, Alex Meyer, Jeffrey Owens, *Using Blockchain for Transparent Beneficial Ownership Registers,* International Tax Review 30 May 2017.

money launderers to provide 'front' businesses through which the proceeds of crime are concealed and injected back into a financial stream. Opacity secured by the 'corporate veil' obstructs ready access of law authorities to the information regarding ultimate beneficial ownership of those legal vehicles and creates conditions where individuals can shield their assets from the tax officials, including proceeds of crime, such as bribery and corruptions. Availability of accurate verifiable information on transparent blockchain-based distributed database regarding the ownership structure, including identification of ultimate beneficial owner can assist law enforcement agencies and tax administrations in identifying those persons responsible for the activity of concern, or who may have relevant information to further an investigation.

Multinationals transacting within themselves using blockchain and thereby allowing real-time generation of local files for audit review, may be relying on the blockchain-based applications to target an intrinsic problem of the transfer pricing[5] – lack of information about comparable transaction between unrelated parties necessary to determine the transfer price.

Linked to the supply-chain management, the blockchain-based applications can be further extended for the use of Customs and Excise. The latter authorities benefit from blockchain in two main respects: the ability to rely on the provenance of the goods transported and ease of sharing the customs related documentation between various departments involved.

For the effective integration of the blockchain-based solutions, however, a supporting ecosystem and a 'whole of government' approach is needed, which includes widespread use of blockchain technologies and the introduction of standards and measures of a regulatory nature, e.g. on the legal identity, which aim at recognizing accounting and tax consequences when booking.

(ix) Decentralized Autonomous Organizations

[5] See also, TY Sim, Jeffrey Owens, Raffaele Petruzzi, Romero J. S. Tavares and Clement Migai, *Blockchain, Transfer Pricing, Custom Valuations and Indirect Taxes: the Potential of the "Trust Protocol" to Transform the Global Tax Environment*, Bloomberg BNA 15 June 2017

Self-executing contracts are creating ways for companies to operate automatically.
Decentralized autonomous organizations (DAOs), bundled smart contracts that are automatically enforced and executed through blockchains, could provide a more autonomous organization.

In the long-run, blockchain technology's most profound impact could be its impact on social values, social and corporate interaction. It is up to taxpayers, tax administrators and advisors to understand this technology and grasp the implications as it evolves.

6. Examples of real-life applications of blockchain-based solutions to date

Swedish land registry, Landmäteriet, is testing private blockchain to register land and properties[6]. The authority believes that technology enables reliability of digital originals of certificates, reduces transaction costs and has superior protection agaist hacking. Similar applications are tested by land registry authority in **Brazil**[7]. On 8 October 2017, **Dubai** Land Department has announced that it is now the world's first official government agency to adopt the blockchain technology to its operations[8]. This is the first real-life implementation of the technology within the framework of the Dubai Blockchain Strategy that intends to carry out all public services transactions on blockchain network by 2020.

China, the world's economic leader, has recently announced its plans to 'utilize technology for social taxation and electronic issuance matters'[9].

[6] https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties
[7] https://cointelegraph.com/news/us-based-startup-ubitquity-brings-blockchain-to-brazils-real-estate
[8] http://www.arabianbusiness.com/property/news/380570-dubai-land-department-to-adopt-blockchain-technology
[9] https://futurism.com/china-to-start-using-blockchain-to-collect-taxes-and-send-invoices/

China is also the first country in the world to test a central-bank backed national cryptocurrency, which is currently being tested in the context of intra-bank transactions[10]. The Monetary Authority of **Singapore** (MAS) is developing blockchain-backed settlement system that aims to streamline cross-border settlement transactions between the banks[11]. Other developments in financial sphere include the Santiago Stock Exchange in **Chile** 'incorporate a blockchain-based securities lending solutions'.[12]

Shipping giant **Maesrk** in collaboration with IBM[13] are developing the blockchain-based solution for **supply-chain management** and documentation exchange between shippers, freight forwarders, ocean carriers, ports and customs authorities. Similar projects are being piloted by **Korean** Customs Service[14].

Estonia, that in 2007 has experienced a nationwide cyberattack, has now transformed into the global leader in the field of cybersecurity, which played a critical role in advancement of the country's eGovernment success though providing a secure non-corruptible blockchain-based electronic personal identity key[15].

Finland is the home of the Futurice, a blockchain application that allows employees to record and get paid for their overtime. Although the application does not interact with the revenue service by withholding and forwarding tax from the salary, the possibilities of using blockchain as tax agent are seriously considered, for example to record information directly from the QR codes printed in the receipts.

[10] https://futurism.com/china-becomes-first-countrchina-becomes-first-country-in-the-world-to-test-a-national-cryptocurrencyy-to-test-national-cryptocurrency/
[11] http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf
[12] https://www.coindesk.com/chiles-largest-stock-exchange-plans-implement-ibm-blockchain-tech/
[13] https://www-03.ibm.com/press/us/en/pressrelease/51712.wss
[14] http://www.koreatimes.co.kr/www/tech/2017/06/133_230428.html
[15] https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4

Rwanda is another real-life success case of a proactive approach to adoption of new technologies. The country has already seen great benefit from digitalization when in 2013 Rwandan government automated business transactions that were submitted in real-time to tax authorities through an electronic system (Electronic Billing Machine). As a result, VAT compliance and collection has increased significantly. Although blockchain applications have not yet been used, government is taking the technology seriously as a step towards further progress.

India[16] has publicly announced its plans to use blockchain-based solution for recording of transactions in real estate. The intrinsic qualities of the blockchain – transparency and immutability – can prove critical in combatting land registry fraud that is estimated to amount to $700m in bribes.

[16] https://www-cnbc-com.cdn.ampproject.org/c/s/www.cnbc.com/amp/2017/10/10/this-indian-state-wants-to-use-blockchain-to-fight-land-ownership-fraud.html

Other FAQs usually asked by the tax ministers and administration

7. Can Access be Restricted on the blockchain?

Yes, apart from the "open" blockchain upon which Bitcoin is based, there can be "permissioned" blockchains where the ledger is encrypted so that only parties allowed to view it may do so.

8. What are the differences between the Bitcoin use of blockchain from other uses?

(i) Assets over Cryptocurrency

Blockchain can be used for a much broader range of assets than just cryptocurrency i.e. as a token-free shared ledger. Tangible assets such as cars, real estate and food products, as well as intangible assets such as bonds, private equity and securities can all be "tokenized". In one business use case, Everledger is using blockchain to track the provenance of luxury goods to minimize fraud, document tampering and double financing. Now, over one million diamonds are secured on blockchain.

(ii) Identity over Anonymity

Bitcoin thrives due to anonymity. Anyone can look at the Bitcoin ledger and see every transaction that happened, but the account information is a meaningless sequence of numbers. On the other hand, businesses have KYC (know your customer) and AML (anti-money laundering) compliance requirements that require them to know exactly who they are dealing with. Participants in business networks require the polar opposite of anonymity: privacy. For example, in an asset custody system like the one being developed by Postal Savings Bank of China, multiple parties, including financial institutions, clients, asset custodians, asset managers, investment advisors and auditors are involved. They need to know who they are dealing with but one client or advisor doesn't necessarily need to be able to see all transactions that have ever occurred (especially when those transactions relate to different clients).

(iii) Selective endorsement over proof of work

Consensus in a blockchain for business is not achieved through mining but through a process called "selective endorsement." It is about being able to control exactly who verifies transactions, much in the same way that business happens today. If one transfers money to a third party, then one's bank, the recipient's bank and possibly a payments provider would verify the transaction. This is different from Bitcoin, where the whole network has to work to verify transactions.

9. Difference between Bitcoin and Ethereum

Bitcoin is a platform for decentralized currency while Ethereum is a platform for decentralized currency and importantly,engine for applications which can be run without a need of trusted third party (some central server).

10. What is a smart contract?

Smart contract—is a piece of code which is stored in the blockchain network (on each participant database). It defines the conditions on which all parties using contract agrees and certain actions described in the contract can be executed if the required conditions are met.

As the smart contract is stored on every computer in the network, they all must execute it and get to the same result. This way users can be sure, that outcome is correct.

11. How does a blockchain transaction actually work?

A typical blockchain transaction works broadly as follows:

1. Transaction initiation: One party (the sender) creates a transaction and transmits it to the network. The transaction message includes details of the receiver's public address, the value of the transaction, and a cryptographic digital signature that proves the authenticity of the transaction.

2. Transaction authentication: The nodes (computers and users) of the peer network receive the message and authenticate its validity by decrypting the digital signature. The authenticated transaction is placed in a "pool" of pending transactions.

3. Block creation: Pending transactions are put together in an updated version of the ledger, called a block, by one of the nodes in the network. At a specific timing interval, the node broadcasts the block to the network for validation.

4. Block validation: The validator nodes of the network receive the proposed block and work to validate it through an iterative process that requires consensus from the majority of the network. In essence, because all parties have the same data set, they validate by ensuring the information matches their ledgers. Different blockchain networks use different validation techniques. Given that the validation happens across multiple peers in the network that compare the information to their own data sets, fraudulent transactions are nearly impossible.

5. Block chaining: If all transactions are validated, the new block is "chained" into the blockchain, and the new current state of the ledger is broadcast to the network. This whole process can be completed within 3 to 15 seconds or even faster as the technology advances.

12. How are transactions validated?

Consensus is the mechanism by which the nodes agree whether a transaction and block is valid or not. As mentioned above, transactions need to be validated by the nodes. Nodes are parties with the ability to vote on the validity of a transaction. There are many cryptographic algorithms a party can use such as proof of work and proof of stake. Consensus rules also require the creator of the blockchain application to determine how many nodes are required to validate the transaction before it's allowed to be completed.

Sources: Adapted from (i) "Blockchain Basics: Q&A for Services Buyers" June 2017 | Authors: Christine Ferrusi Ross, Research Vice President, HfS Research; Reetika Joshi, Research Director, HfS

Research (ii) https://medium.com/startup-grind/gentle-intro-to-blockchain-and-smart-contracts-part-1-3328afca62ab (iii) https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html (iv) https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html (v) https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/