UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Conversion in IT

Kristin Sõgel

Distributed Ledger Technology and External Mandatory Reporting in Banking Industry

Master's Thesis (15 ECTS)

Supervisor: Fredrik Payman Milani

Tartu 2018

Distributed Ledger Technology and External Mandatory Reporting in Banking Industry

Abstract:

This thesis gives an outline of the potentials to attain time and cost effectivity to all partakers by using distributed ledger technology, including blockchain, in the mandatory reporting process executed by credit institutions to relevant authorities regarding financial crime and cross-border tax reporting with globally effective diminishment of these illicit transfers.

Keywords:

Distributed ledger technology; Blockchain; Mandatory reporting; Banking industry; Financial crime; Compliance

CERCS: P170 Computer science, numerical analysis, systems, control

Hajutatud andmebaaside tehnoloogia ja pangaväline kohustuslik raporteerimine panganduses

Lühikokkuvõte:

Uurimus käsitleb kõigile osapooltele aja- ja kuluefektiivsuse ning globaalselt illegaalsete ülekannete vähendamise saavutamise võimalusi, kasutades pankade kohustuslike raporteerimiste protsessis asjaomastele asutustele finantskuritegude ja piiriülese maksuinfo teavitamisel, hajustatud andmebaaside, sealhulgas plokiahela tehnoloogiat.

Võtmesõnad: Hajutatud andmebaasid; plokiahel; kohustuslik raporteerimine; pangandus; finantskuritegu; vastavuskontroll

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine

Table of Contents

1. Introduction

Background

Banking is one of the most regulated industries in the world. The growth of various type of regulations commenced after the last global financial crisis in 2007-2008 to enhance the monetary systems' stability and reduce the future negative impacts on it. Regulations steadily evolved, beginning from imposing post-crisis liquidity standards, capital adequacy and solvency regulations, demanding higher capitalization requirements from banks.

There is no sign that the needs and demands from the monetary environment may be decreased - the number of regulations growth [1], by creating new or changes to existing ones, gross up globally to ca 200 changes per day [7, 10]. Moreover, previously only local demands have now expanded into cross-border obligations and not abiding them is not an option due to several accompanying fines, possibility to lose the trust of clients, partners and banking licence. Hence the immensely rising appetite of the regulators is understandable approach and directly correlated with the bank's growing burden of analyses, assessments and reports to be created on the internally and externally gathered data, the imposed fines and more stringent rules do not seem to mitigate the existing problems - slow adaptation of current systems to catch criminal activities effectively on spot.

The credit institutions cannot neglect any of the imposed reporting or adequacy duties and are obliged to find means to bear them. But as the accompanied compliance costs are not related to any specific product or service and cannot be therefore recuperated directly from the client as legal consultation expenses on loan agreement could, they do not create any direct profit for the bank.

The expenditures expand when specialization of the bank involves cross-border client base because the regulatory compliance requires not just barely knowing and following international laws and regulations but executing more enhanced interactions with applicable authorities and additional frequent verification process driven communications with international clients. This cannot be performed without the sustainable and advanced IT systems. According to Gartner's research the forecast for credit institutions' IT costs are estimated to be globally US$519 billion in current year [24].

By now formerly pure prudency has gradually grown into administrative crime spotting burden necessitating daily verification, monitoring and screening of customers and counterparty data, accompanied with the pertinent all-embracing reporting to various authorities. To conform with all mandatory requirements banks had to employ specialists, compliance officers, who ensured that the enterprise followed all relevant and necessary laws, regulations, directives and guidelines in duly manner and on time. To express the immensity of the problem - every medium bank in Europe had to input 200 full-time specialists to work [3] to comply with just one regulatory norm - the banking prudential regulatory reform introduced to set minimum obligatory standards for international credit institutions - Basel III [2]. The growth in employment costs has been similar all over the world - according to Federal Financial Analytic research [4] the compliance costs in the United States have risen double comparing expenses in years 2007 and 2013. The responsibility for execution of all regulations in many jurisdictions is personal, which means that the compliance officers can be held personally liable, accompanied with enormous personal and institutional fines, if the credit institution they are responsible for fails to perform its obligations.

The afore mentioned would be not necessary without the core focus of banking – the customer, from whom the changed banking requirements to observe the anti- money laundering

and counter terrorist financing prevention demands several tedious and time consuming specific interactions, verification of owners, proof of funds, business plans and counterparties. This process is somewhat similar and yet different in every bank the client has an account in but yet cannot be simplified or unified due to the existing diversity of legal requirements and state's capabilities across the regions. This has led to, as shown in the Thomson Reuters' double survey on financial institutions and their corporate clients [6], to drastic reduce in customer experience as the involved paperwork in customer due diligence was too burdensome and accompanied with noticeable rise in expenses which on average was US$60 million annually per financial institution with peaks up to yearly US$500 million for some institutions on these obligations only.

Besides regular technology development and labour expenses inside the bank, regulatory fines (in addition to the personal accountability and enormous fines against the responsible officer) upon defaults in complying with the regulations also may apply. These fines in their size can be enormous. For instance, to only one bank, the Deutsche Bank, for insufficiently following anti-money laundering regulations between 2011- 2015 the fines total size of US$600 million were issued by the United Kingdom Financial Conduct Authority [16] and the New York State Department of Financial Services in the United States [17] during 2017. McKinsey & Company has analysed the SNL Financial data and found that the operation income of 20 large US and EU universal banks has decreased by 10 % over 2009 – 2014, when the imposed regulatory fines have been growing almost 45 times [25]. Consequently, the costs on IT development and compliance employment are vital for avoidance of the fines and prevent the possible forfeiture of trust of customers and authorities or even business.

Considering the aforementioned, it is not hard to foresee the escalations of future problems banks will encounter as their once costly sophisticated core systems with built-on attachments and paper-based client interactions will fail to serve them well in the new complicate and challenging ecosystem of e-money, cloud-storage and distributed ledger technology.

Concisely, the overgrowth of regulative burden, that involves collecting, verifying, analysing, assessing and reporting particular customer data to the authorities, is distressing the credit institutions by (i) cumulating operational costs due to required IT investments and maintenance, (ii) creating lower customer satisfaction due to more extensive and expensive due diligence process, and (iii) risk of high fines in case of non-compliance; while the actual goal is to hold banks responsible for gatekeeper tasks for spotting and stopping money laundering and tax evaders.

Problem Statement

The regulatory challenges banks encounter can be divided into three major areas that share similar grounds or purpose. First, are reforms which involve any kind of protection - assets or customers wise. These cover consumer and capital market protection, capital liquidity and resolution plans. Secondly, required standardization that incorporate the governance, consolidation measuring and statistics. Thirdly, and most challenging is the area of reporting, that involves accurate data on continuous monitoring of customers and their counterparties interactions, which formulates into applicable financial and crime reporting.

Within the domain of regulations there finds two areas of reporting and the functions necessary for their correct execution. The first, financial reporting incorporates forms of statistical reporting that specifies besides numeric values customers' name. This includes reporting to supervisory authorities on credits, collaterals, debts and deposits as well as local or cross-border change of tax information. Secondly, the financial crime that involves customer due diligence, monitoring of customer's pertinent activities to provide timely and

proper information of made findings to authorities (tax, supervisory, police, etc) for them to require more proof to find out and judge those customers or their counterparties who are engaged in illegal or suspicious activities.

The distributed ledger technology or DLT, which also includes its sub-category - blockchain [5], has shown that its incorporated functions may appear as a potentially efficient game-changer to defeat the current obstacles in attesting trust across the borders. Many bank consortiums and authorities have closely followed this development and are already investing heavily in understanding how these technologies could be of use for dealing with payments, treasury, securities, confirmations and compliance to regulations. Current focus has been more on the technology's essence itself rather than how this could improve processes of the credit institution.

Therefore, in the light of the above context, the research question of this thesis is to explore how the distributed ledger technology with its subcategories, can innovate the compliance processes of the banking sector, provide new ways to securely overcome the banking industry's challenges in external reporting which are grounded on customer data and in unison improve the interaction experiences of customers and authorities to achieve the ultimate aim avoiding the states and banks being used for money laundering and terrorist financing, collect more taxes and progress honest economy.

The structure of this thesis by chapters is as follows:

In the first chapter the background of the compliance and area challenges in the banking sector is conceptually outlined. It incorporates the explanation of the core of the banking compliance, involved terms and definitions, applicable regulations, requirements and challenges together with the possibilities the distributed ledger technology (including blockchain) offers. The second chapter describes the current state and dependencies the average universal bank and its counterparties from customers to authorities encounter concerning customer due diligence, screening, monitoring, analysing, and crucial external reporting. The third chapter presents the analyse of the articles, researches and ongoing projects available on this relevant or similar issues describing how scientists and technology have and could solve these challenges and what obstacles they have encountered. The forth chapter provides the analyse of the solution to the necessary alterations of the current procedures with the aid of distributed ledger technology to advance the involvement in and quality of the process under surveillance effectively and securely for all parties. The fifth chapter outlines the discussion with founded opportunities, limitations and further possibilities.

2. Background

This paragraph will introduce the background of the area challenges, current ways and activities to accomplish intact with the concept of compliance and possible future measures to manage them with the aid of DLT.

Area challenges

The global financial environment (including Europe, Asia-Pacific, United States) has similar regulatory challenges for all credit institutions, outlined by FATF [33] mostly in eight areas:

1) Financial crime - that include anti-money laundering and combating terrorist financing (AML/CTF) together with know-your-client (KYC), beneficial owner (BO) and/or ultimate beneficial owner (UBO) confirmations and several forms of customer due diligence (CDD) according to Financial Action Task Force (FATF) or Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval) standards that endorse global AML/CTF measures based on technical compliance and prompt reporting;
2) Financial reporting - based on Basel III Pilar 3, International Financial Reporting Standard (IFRS 9), Foreign Account Tax Compliance Act that orders credit institutions to collect and report taxable data and if necessary, withhold and transfer taxes on US citizens (FATCA); similar aim to enhance taxation among member states of the Organisation for Economic Co-operation and Development (OECD) has stipulated to Common Reporting Standard (CRS), Basel Committee on Banking Supervision and many more;
3) Consumer protection – includes the OECD introduced basis for data protection [76] and protection of any kind of client's rights such as deposit insurance and financial advice;
4) Capital markets reform - involves market integrity, derivatives reform, capital markets integration, consortiums against shadow banking;
5) Capital and liquidity issues - like stress testing, higher minimum capital requirements to improve the stability of the area;
6) Resolution planning – that help to avoid vast damages in case the bank faces the insolvency;
7) Risk transformation – as measures like corporate governance and risk management strengthening together with the controls and regulations on outsourcing and basic technology rules;
8) Structural reform – as all the above involves different standards and data transfers, the standardization of numerous requirements (scope of business, priority sector targets, consolidation measures) is also necessary.

This thesis will focus on the first two and data protection from the third challenge, which are interacted with each other very closely as involve the vital grounds for understanding the business and beneficial owners of the clients, analysing customers' regular business by daily monitoring and screening the payments of customers and their counterparties to aid fighting and catching criminals and funds incorporated in money-laundering, corruption, fraud, tax evasion or terrorist financing schemes while protecting the data according to the legal regulations.

Evolvement of compliance function

To accomplish the above task in a structured and controlled way and stemming from the wish to "enhance the sound practices in banking industry" [26, 7] the Basel Committee on

Banking Supervision, which members are central banks and supervisory authorities, introduced in 2005 [26] a new function, called compliance, inside the banks. This new function was to ensure all banks activities to be in compliance with applicable laws and regulations by identifying existing risks and implementing ways to mitigate them.

At the beginning the compliance function could work together with the audit and delegate it's tasks to that function. But with growing globalization and technology that allowed cross-border high speed and automated payments the task forces responsible for prevention the money laundering and terrorist financing introduced gradually heightened requirements for banks. The latter was set out partly because the banks had the overall information on the clients and their regular behaviour and payments and partly because the state authorities did not have themselves grounds and resources for receiving and analysing that data. Consequently, originated from the need to prevent money laundering and to aid following the set sanctions, the banking sector was strongly recommended to implement in their practices the risk management system's model of three line of defences. In this model the compliance is responsible for the second line risk alignment controls over the acts of the operating management and business, which act as the first line. Internal or external audit provides leverage and independent validation of them both in the third line, requiring proof of activities from previous two line of defences.

The essential of the compliance function has remained intact – to be the core risk management of the bank accomplishing its business goals using available the systems in a lawful manner. Stemming from the above the credit institutions are required to set their risk appetite in conformity with their possibilities managing the business without endangering the institution, clients, their funds and all relevant counterparties and compliance function should ensure that these risks are properly assessed and mitigated.

Customer due diligence during onboarding

The essence of banking is the customer. To mitigate the accompanied risks, the CDD process must be executed by the bank to identify the customer, inevitable relations or interest with the bank's region of activity, their ownership, business structure and relations in order to assess their suitability with the bank's risk appetite to prevent money-laundering, terrorist financing and other fraudulent or criminal acts. To start the process of opening the bank account, the original documents or notarized/apostilled/translated/digitally verified copies need to be gathered and presented to the chosen bank together with necessary authentications of representative rights. In many regions the personal identification of the client by the bank official is a necessity.

This is known as know-your-client (KYC) process that forms a part of CDD of every bank and is executed in the form of meetings and questionnaires answered by the potential customer and accompanied with compulsory verified documents. Each bank is required to perform interview, check the filled KYC answers, verify their content against applicable registries identifying the applicant and ask more questions to specify the background of more profoundly. Necessary data should be inserted into the banking system to firstly assess the associated risks applicable to particular client, its owner of funds (UBO or BO with the ownership per centage different per region), business industry, geographical and political factors and from that score make the analyses to actual decision of onboarding or declination.

According to Thomson Reuters Survey on KYC challenges in 2017, the onboarding process may averagely take nearly one month [27, 10] - all to effectively (and very often, not) onboard the customer. As the forms require more input from the customer, the time they

spend on onboarding, is averagely 5 days longer than for banks [27, 10]. The same Thomson Reuters KYC Survey has found that the average global number of contacts by the bank toward the corporate customers during onboarding is twice as high, 8 times, as for average for all customers (4 times respectively) and as cross-border companies have in an average 9 different accounts in banks all over the world [27, 11], it is possible to see the overwhelming burden that lays on the customer as well than on the banks. In some regions the banks are obliged to report authorities the declined customers with applicable reasoning.

During service

After successful onboarding the frequency and content of customer interaction is dependent on the customer's actual business risks. To accomplish assessment of those risks, the credit institution is obliged to screen all customers and their transactions parties on daily basis against relevant sanctions lists not to accept or send funds to restricted persons/organisations/countries, to monitor customers' payments and actual financial behaviour against the estimations stated in KYC. The customer is regularly contacted if bank's investigation shows ambiguities, if their data and or their UBO/ BO possession changes or if their KYCs or various forms or proofs of tax residency require updating. Such requirement does not apply to listed companies. Renewal of KYC is a regular obligation. The bank initiates this process prior the KYC's validity term and upon spotted signs of deviations visible in registries, business pattern, geographical activity and ownership. In the latter cases the customer also is required to promptly notify the bank and documents completed at onboarding will be refilled, verified and exchanged again.

Interactions

The core of the reporting obligations is knowing the banks' customers governance, origin of funds and business relations as precisely as possible. CDD process as continuously changing, requires unceasing back and forth interaction with all the counterparties, signing documents and checking the collected data regularly, verifying and inserting the gathered data into banks databases. Besides above responsibilities of the credit institutions, the combating money-laundering and terrorist financing (AML/CTF) regulations also places burden to all banks' customers who are themselves obliged, before entering into the business contracts, to assure that their counterparties are not engaged in any criminal activities. In this challenge the clients currently mostly rely on the systems, analyses, screening and monitoring of the banks they use for banking, hoping that banks would buffer their business against offenders. Correspondingly to banks, the customers can be held liable as well if their due diligence on their business partners is found insufficient by the authorities.

It is challenging also to authorities like, Financial Crimes Enforcement Networks (FinCEN) and Financial Intelligence Units (FIU, hereinafter together FIU), a special government agency (separate or part of police) that analyses the received suspicious activity reports (SAR, also known as Suspicious Transactions Report) from local banks, other similar units of affected countries and investigates the crimes related to money laundering and terrorist financing, tax evasion and other similar fraudulent acts or attempts, especially when the scale of the scams is global and requires swift actions to successfully trace and freeze criminal assets. Ensuring the accuracy of law and order the authorities (including police, tax department) may require additional *ad hoc* and more in-depth information from the banks on their policies, their customers or the deals they investigate. In these cases, bank bearing the banking secrecy, has to gather and reveal more *ad hoc* data on this particular matter and as criminal law may be involved not reveal existence of the enquiry to client.

The scale of this task is global, as credit institutions, their customers and controlling authorities in all countries have the same challenges and obligations to serve in a trustful, secrecy protective and by correct way and means. To accomplish the latter the counterparties have been using several impartial intermediaries or bank-to-bank companies and country-based verification agencies or persons (notaries, sworn translators, local representatives, attorneys). These third parties may all use different and not well compatible technology within the country or region, but majority of the cross-border original or verified document sharing in CDD is done still on paper. These papers are kept within banks, oftentimes digitally duplicated for security reasons and for swifter response to *ad hoc* inquiries to FIUs.

Distributed Ledger Technology

The Distributed Ledger Technology (DLT) incorporates many features that may aid overcome the trust and verification problems existing in banking industry reporting requirements. According to the World Bank FinTech Note No 1 DLT "refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers)" [30, V]. This technology permits recoding and sharing of information in any form of data (numeric, binary, alphabetic, characters, etc) computer files (ledgers) in a unified (distributed and/or shared) way with all or certain participants of that database network. Beside previous access network, other added functionality layers can make the network more adaptable and flexible. With the aid smart contract program more data, like contracts, confirmations, may be added in the form of layers (contract layer) to the existing DLT network. Also access rights can be determined to certain chains (control layer), network communication rules (communication layer), validation and verification instructions (consensus layer) and the form of acceptance of the core (content layer) addressed to the whole network [32, 10].

The ledger can also be a permissioned type which would be run by a single or multiple consensus parties and which insertion rights are held by only certain participants [32, 9]. These partakers are, to the contrary to public ledger, identified and known to other participants and the validation process does not require as much of verification in the consensus protocol as the public one. Private ledger could be used within a company or group of companies all over the world. As decentralized public approach necessitates for confirmation of trust the proof of work, the permissioned and centralized one, which is in control of its developers/owners, does not necessitate this type of proof because the members are joined only with approval and do not require extra trust from all joined members for every deal.

The benefits the use DLT would provide is the rise in efficiency to all users, improvement of trust, security and swiftness in exchanging, verification, recording or reporting of data or actions with them. DLT would also enable "management of digital identity through public key cryptography" [31, 7].

DLT is a broader term and has several subcategories created over the years. Blockchain, being the most investigated eminent subcategory of DLT, is a basic for cryptocurrency named Bitcoin [64], being probably one of the most known technology that uses DLT and blockchain "in which the ledger comprises "blocks" of transactions" [31, 1] and with peer partakers blocks joins in a form of a chain of verified links. Bitcoin, the first version of blockchain, enabling ownership and trade of digitized currency for deals over the internet, is run on public (permissionless) ledger allowing anyone pseudo- or anonymously to participate with equal authority being an integral part of verification. The higher the number of participants, the pricier in energy consumption and costs is the consensus verification mechanism (proof of work, proof of stake, Byzantine) [89, 4] of the public ledger. The difference of blockchain is the feature that the content of inserted data can be only add-on, it is verified

by all required partakers, approval is fingerprinted with hash - an "authenticated by a cryptographic signature" [31, 1], incorporated via technology to all other members past and future ledgers and therefore cannot be changed without the consent of all or certain participants in real-time over internet. Verified block form an add-on chain conforming as a whole a trusted and open system. Therefore, the information stored on blocks is available to all partakers and the protocol, assuming the honesty of all partakers, incorporates the possibility that 51% of power owners of that chain could take over the system and reverse previous transactions [101].

Besides blockchain, also newer forms of DLT have been invented to overcome the current performance slowness, expensiveness, inefficiency [91], "scalability, flexibility and governance" [86] problems accompanying so called vertical blockchains. Such new ones are Directed Acyclic Graph (DAG) elik Tangle, an open source DLT where transaction verification and proof or work is more vertical nature, simplified and quicker [90] or patented private ledger DLT on Swirlds platform using for consensus a new method called Hashgraph [99] receiving consensus with dispersing information to haphazardly selected partakers in the form of "gossip and virtual voting" [75].

To regulate the growing DLT (including blockchain and other), there are missing regulator's governing protocols and laws, as this technology is in early implementation, but the existing requirements on security and privacy apply to any of the systems used, including DLT where this is the case. But steps to achieve that have been taken by International Telecommunication Union on interoperability of DLT [93] and for financial services the Standards Australia has introduced roadmap on blockchain [92] as step to issue standard ISO/TC 307 for DLT and blockchain. Currently there is no unified agreed exact "criteria for determining what counts as a blockchain and what does not" [37,4], in order to distinct form cryptocurrency and focus on regulatory technology and solving the goal to combat fraud, in current thesis DLT term is used in a broad way to include all factors necessary for secure, immutable, traceable, scalable, stable and trustworthy regulatory reporting whether in a view of block or chain or not.

By 2022 the projected infrastructure cost saving upon implementing the DLT in banking industry would be "between $15-20 billion per annum," as estimated by Wyman [1, 15]. Most known public distributed ledgers according to the World Bank [30, 14] are Bitcoin [64], Ethereum [65] and Litecoin [63] and of permissioned private distributed ledger is Hyperledger (found by Linux) [66], on grounds of which several technology companies and themselves or with collaboration of consortiums of other institutions have developed different proficiencies offering platforms like Hyperledger Fabric (by IBM) [67], Ripple [68], Sawtooth Lake (by Intel) [69] and Corda (by R3 CEV), presently the most known decentralized DLT database platform [70]. Many of the latter announce incorporating consortium approach for attaining consensus [89,8]. Some of their possibilities are discussed in the next chapter.

Parties effected

It is hard to pinpoint exactly how many banks, persons and companies are involved in total, but some picture could be drawn from the data available. According to the World Bank notice based on the International Monetary Fund's Financial Access Survey 2016 the total number of the licensed banks and their customers globally is not very certain, aiming to more than 12,5 banks (including branches) to 100 000 adults in 2016 [8]. According to the global measurement of the financial inclusion, measured by the World Bank in their 2014 survey [9], there are 2.24 billion private people, equalling to 62 [9, 4] percent of the adults of the world, who have a bank or mobile money account. According to the World Bank there

are 43192 [10] listed companies in the world in 2016 with total market capitalisation of US$64,853,776 million [11]. Regarding the number of smaller enterprises, it was according to the gatherings in 132 countries by the International Finance Corporation (World Bank Group) reports in 2010 that on average there are 31 enterprises per 1000 people [12, 3].

3. Current state

3.1 Statutory Background of the Customer Due Diligence

The aim of the CDD process is to follow relevant international regulations and standards that necessitate banks to know and verify their customers from their identity, ownership, activities, counterparties, business relations and transactions to source of funds. Nevertheless, their differentiations in their necessary reporting outcomes, the analysing methods of substantiation of the data for these reports has in many countries been left for the institutions to decide. Therefore, in this thesis, the Financial Actions Task Force (FATF) recommended risk-based approach (RBA) guidelines of the banking industry [33] regarding activities in the anti-money laundering analyses, which allow the banks to assess and mitigate their accompanying risks, form the basis of the process descriptions. FATF "is an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction "[29]. Their guidelines are issued in the form of recommendations to countries authorities for ensuring that the institution under their supervision follows these rules and prevents criminal activities with the aid of their systems.

Firstly, one aim is to prevent processing transactions to counterparties against whom enforcement acts have been imposed and therefore with whom the banks are aimed to block financial interactions. The Office of Foreign Assets Control (OFAC), the division of State Treasury of the USA, is one of the entity that sets out sanctions against persons, companies or groups who are "owned, controlled by, or acting for or on behalf of, targeted countries" [28]. Specially Designated Nationals (SDN) are exactly those persons, companies or groups against whom any sanction has been set. Their names are gathered in continuously updated watchlists against which the financial institution must screen all their clients, payments' counterparties prior execution the transfers to find and verify actual hits and block such accounts or freeze payment funds and report accordingly to authorities/FIU in the form of SAR. Globally there are many other sanction lists (United Nations Sanctions, Australian Sanctions, UK Financial Sanctions, EU Financial Sanctions to name a few) besides OFAC, which all are obligated to be screened in relevant countries as it is not allowed doing business with prohibited SDNs. Frozen funds should be kept unattainable for the SDN and transferred only upon relevant authority's order. The client may be notified of such freeze and claims release from authority. Besides SDNs there are other different hits like politically exposed persons, their relatives, debarred parties, most wanted lists and similar. These hits should be as well evaluated, spot valid matches (name, birth date and place, nationality, ID, etc) and reject payments, if applicable.

Secondly, the target is to be aware of the unusual activities via transaction, behavioural and typology-based monitoring among the executed payments of the customers, investigate the findings and escalate them accordingly based on their normal business and KYC estimates. The reporting outcome of this RBA classifies as reporting of financial crime (AML/CTF, suspicious transactions, etc) promptly after analysed and spotted in the form of SAR to FIU for investigate findings. The FIUs are performing also *ad hoc* investigations inside the banks on client's transactions and their proof, based on applicable scenarios, suspicious actions and patterns. Financial Supervisory Authority (FSA), a local authority which issues licences for and controls over the financial institutions within their region, performs regular and *ad hoc* checks to verify that their supervised banks procedures and actions are in compliance with all compulsory laws.

Thirdly, the regulations which demand collecting, verifying and reporting of precise facts depending on the outcome of the analysis versus the requirements on mandatory dates, also apply. In current work into the latter category the international tax related reporting, is positioned. First includes finding the persons of the United States of America (U.S. or United States) among clientele and their UBO/BOs and based on the grounds of international intergovernmental agreements collecting and reporting taxable data and if necessary, withhold and transfer their taxes to the tax authority. The core idea for the U.S. is to get on hold of their citizens taxable assets located outside. Reporting is handled according to governmental agreements via local tax authorities or directly to United States revenue service institution. Reporting institutions (not limited to banks) are obligated to find out (currently without U.S. authorities help) on continuous basis stated possible indications that refers to the U.S. origin of private or corporate customers and their UBO/BOs, receive applicable verifications and filed tax forms via customer.

Fourthly, similar obligation, but with different thresholds and without the withholding obligation of payments is applicable in banking reporting according to the CRS, stipulated by OECD which aids its member countries to unravel shared obstacles and problems, to pinpoint their citizens (including companies and their beneficial owners) taxable assets outside their regular tax country. This regulation is obliging banks to find and pinpoint on OECD member state tax residents in cross-border tax information sharing project. It was introduced to accomplish the similar purpose to member countries as the United States intended with their FATCA.

Finally, to comply with the preceding demands, the banks require systems, procedures (CDD, screening, monitoring, assessing, etc), analyse tools and quality data verified on various levels (clients, their UBO/BOs, local and international authorities, intermediaries, etc) to preserve their clients' and regulators' trust, data quality and lawfulness of business.

3.2 Customer Due Diligence Process

In the society where banks, in order to perform their CDD, have the possibilities to communicate with the client, state registries and intermediaries via electronic or postal services/means and to assess the risks internally by electronic management from onboarding till termination of the client relationship, the typical and simplified internal workflow of CDD by Oracle [8, 10] on Figure 1 comprises of below.

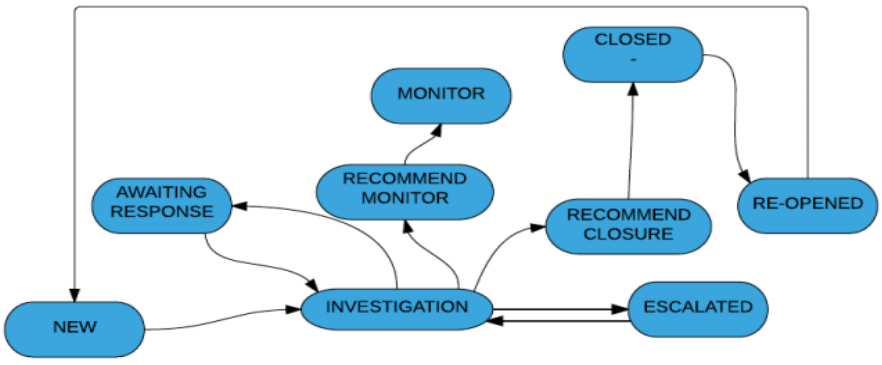

Figure 1. Oracle Know Your Customer workflow

Potential customer risk rating

The RBA approach primes to the applicably risk-adjusted CDD in accordance with their set business risk appetite and assessing potential customers, upon their such request or prior

entering into the business request offering, before onboarding. In order to set the right target, all customer provided documents and filled applicable questionnaires must be checked via state registries, trusted parties confirmations and all watchlists like different international sanctions, embargoes, business relations with sanctioned persons or with national and international politically exposed person (PEP - person who through entrusted/access public/political power could influence companies in order to benefit from corruption and their close family members and associates) as the business relations with sanctioned persons are forbidden and any such attempts or changes must be spotted, stopped swiftly and reported to FIU. If PEPs are involved, either directly with any position engaging decisive or beneficial power or via close family members or business activities and partners, the risk of this customer automatically becomes high. This or any other risk class increase requires more frequent and scrutinised checks and verifications of that customer stated as the enhanced due diligence (EDD) and in some regions also increases as inherited risk the risk-level of all related legal entities and privates. Each RBA institution regulates their onboarding and upon refusals many countries require reporting with rejection reasoning to authorities on regular basis. After considering potential customer suitable for onboarding, the CDD process in its entirety may start.

The below Figure 2 is to reveal on the low level of detail the average dependencies of the CDD process for non-financial corporates regarding data verification, as this requires more analyses and substantiations than the private person's account opening.

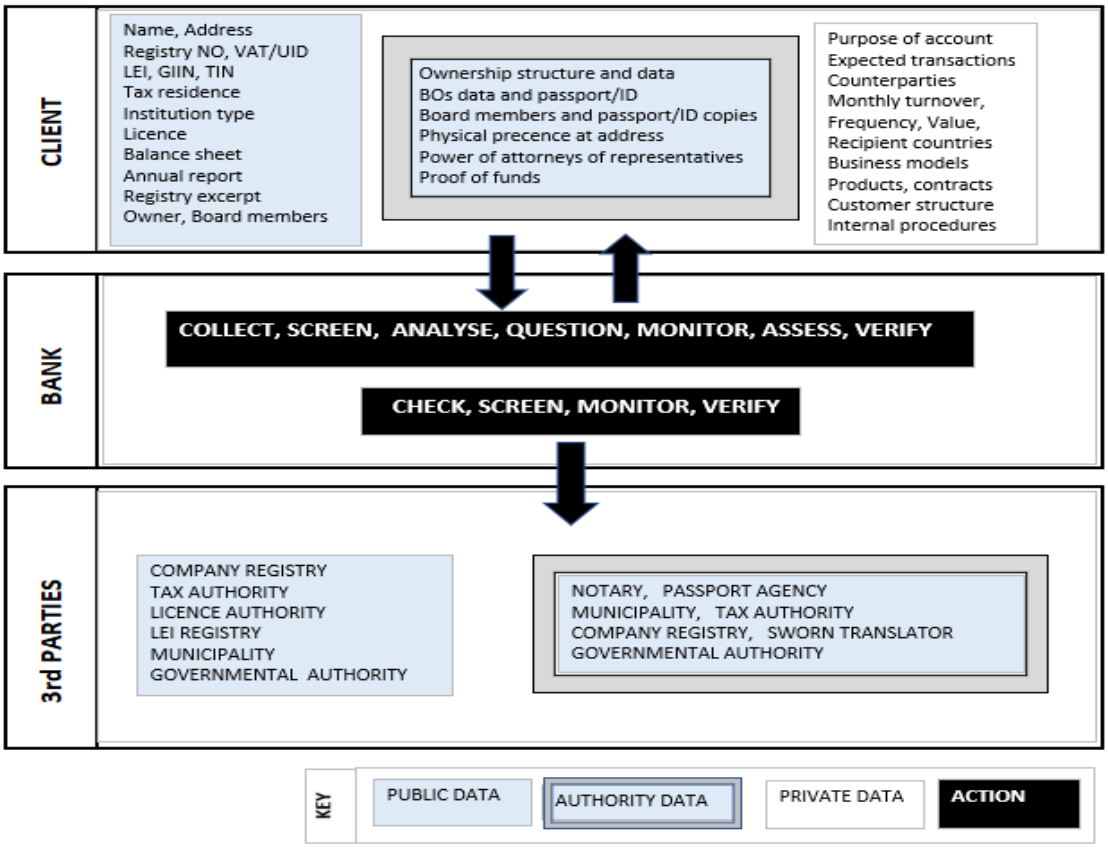

Figure 2. KYC dependencies

It is shown that roughly 2/3 of the information the company needs to present to the bank, is already in some form existing in the state-related or controlled entities and banks act just as collectors and controllers who need to evaluate this data and question the client in case of

controversies and preserve this all in an attachable form for future presentations to regulators. One third of the information necessary for proper assessment comes directly from the client in the form of plans, estimations and data on their counterparties and related contracts. This combined with the gathered verified public data and results of the analyse is valued against the bank's risk appetite scoring model.

The bank is obligated to evaluate the inherent risks of the customer's ownership structure, industry sector, origin of assets and business plans, hazards deriving from the geographical risk if their business, counterparties or owners or their close persons are PEP, sanctioned or origin from countries or regions identified as not having effective AML/CTF systems in place and how this all incorporates with the required services and products offered and channelled by the bank. All these findings and responses are stated in the scoring model associating the clients' business risks according to linked risks and is part of the customer risk rating (CRR) model.

The bank is required to assess and value all applicable risks as a whole, control and deliver an operative level of mitigation and refuse (and report) customers which direct and relational risk they judge not acceptable for bearing. The more publicly controlled the information about the customer is (listed companies), the lower the level of obligatory controls for credit institutions, as the control function is shared with the authorities and all parties exchange relevant data via extensive reporting. The younger the company, non-clear the business plans or vaguer and non-transparent the ownership structure, the higher the risk. Many risks are also inherent, so for instance if the BO of the company becomes PEP, the company's risk rating is automatically revalued. Depending on the risk associated with applicable customer, the CDD process must be repeated regularly conditional on the stated risk rating or if any notification of the change or anomalies from estimations occur. If the customer is offering financial services and is therefore controlled by the respective regulatory authority, the information necessary for CDD is more extensive. In this case the same regulator has already at his disposal the expert data (not public) on particular licenced institution and the onboarding bank is just verifying this via the financial service providing customer.

Similar as shown on Figure 2, applies to the private persons, but with small deviations - instead of balance sheet the differentiation of incomes is required, and the details mandatory for the corporates (business model, annual report, offered products, internal procedures) are not necessary.

If bank is involved in the business with international clients, the capacity of tasks and risk rate rises as the verification and control methods are more uncertain and require more trusted 3rd party proof of the background and lawfulness. The same applies to the client who is required to notify upon any required changes all relevant authorities and banks in all states they engage in with business. Reports under study in this thesis all origin from the KYC process.

3.3 Anti-Money Laundering Process

The knowledge of the customer's business, ownership structure and counterparties is required to map customer's regular actions, estimated typical behaviour and spot any deviations or abnormalities thereof. Among deviations the bank is obliged to identify these uncommon activities that may indicate a lead to money laundering, terrorist financing, fraud, tax evasion or crime, investigate these with due care, ask the customer to provide clarifications and proof of the lawfulness of those activities, counterparties or funds. If the analysis of performed investigation does not verify the legality of these activities or the customer refuses to deliver information, the bank is obliged to report this, without the customer's

knowing, in form of SAR to the respective authority (FIU, Police) with accompanying documents - application, proof of analysis and investigations, account statement, signed agreements, to name few.

Figure 3 displays the dependencies in data sharing in AML process. The data collected by the bank in the CDD process is ranging from publicly available and known by authorities, to private business plans and estimations provided by the customer itself. The risk assessment made on this knowledge and estimations is essential and this may alter due to behavioural, geographical or any other relevant changes throughout the regular banking of every customer. The actual transactions, financial activities and their counterparty data executed via the bank is also considered private data not available to others. This data reflected through oftentimes compulsory scenarios stated by the local regulatory, FIU or other authority, risk assessment patterns and watchlists that using screening and monitoring tools-systems aid discovering particular customer's abnormalities and suspicious transactions to prevent, seize and report illegal funds and activities effectively and promptly.

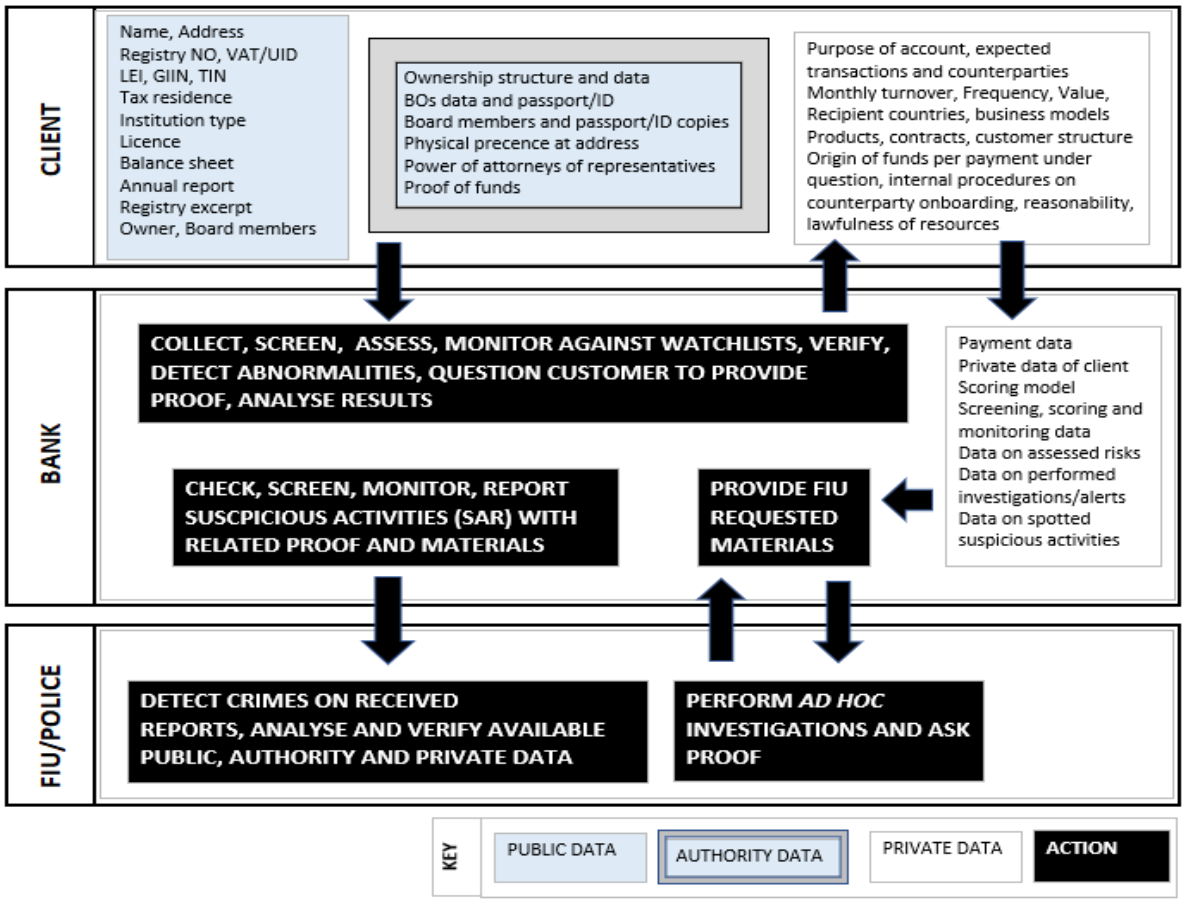

Figure 3. AML/CTF reporting dependencies

Bank's obligation is to guarantee that all payments to SND customers and SND transaction counterparties are blocked and reported in SAR form. Same applies to all transactions that are made to, from or through the bank, and are for instance unusual for particular customer, to which the customer has not provided evidence or proof, which have large volume in bulk or in parts or which the banks know, believe or has reason to suspect criminal activities like money-laundering, terrorist financing or any fraud or crime. All systems involving the screening and monitoring of customers and their all transactions within the bank, their modelling algorithms and techniques to spot alerts on transactions that require investigation,

need to be validated regularly by the bank. All investigations, as CDD and risk assessment and rating, require proof of trail for audit, compliance or external SAR or *ad hoc* reporting. SAR reports must be accompanied by the relevant agreements, customer data, account statement and all proof gathered during the investigations. FIUs who receive and analyse SARs and FSAs who regulate and supervise credit and financial institutions cooperate closely across the borders and are therefore highly informed of suspected crime, persons and companies who are under investigation or suspected to be engaged in financial crime, upcoming financial crime patterns in certain regions of the industry and developing measures to prevent this financial crime. While banks have to rely on their gained experience, knowledge and sometimes gut feeling and still can observe only small piece in the puzzle.

3.4 Tax reporting to the United States

FATCA external reporting dependencies laid out on Figure 4 depict the workload of banks necessary to correctly follow the rules stated in the intergovernmental agreements. Banks, as financial institutions, are also obliged to register oneself with U.S. authority, discover and report year-end-basis the customers, their BOs and funds originated from the United States either directly to the IRS or to their local tax authority according to FATCA.

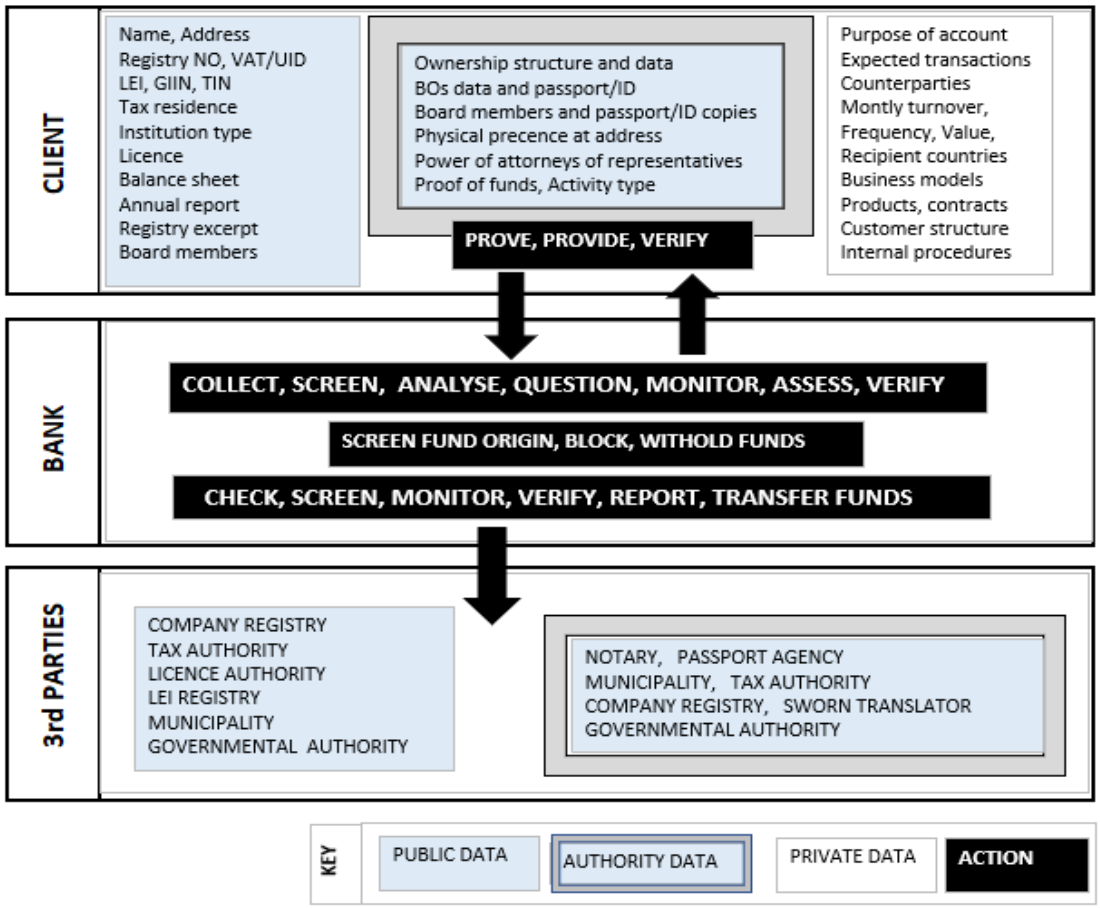

Figure 4. FATCA external reporting dependencies

The actual reporting is based on the bank's findings on relevant information related to the United States, called U.S. indicia. The latter is not complicated when U.S. indicia is deriving from the client's assured tax residence, address or ID, but more challenging when the same has to derived from e-mail, phone or place of birth. Different thresholds and criteria apply for evaluating the business types, reportability volumes and reporting. The level of investigations of KYC of trust corporations is more intricate and requires special analyse for

FATCA reporting purposes. The customer with spotted U.S. indicia has to, upon bank's request, provide the bank with self-certification of its financial activity, different Internal Revenue Services (IRS, U.S. tax authority) signed forms to avoid withholding of tax rate from all U.S. originated funds, transfers and received interest or dividends on U.S. assets. In case the customer fails to provide proof within 90 days, the bank is obliged to withhold all funds the customer receives from U.S. sources. As the latter is very difficult to pinpoint and the fines for non-compliance are hefty, many banks refuse or have the right to close account, if the client is or becomes a FATCA reporting person. Listed companies are exempted from FATCA reporting as their financials are public already.

3.5 Tax reporting to OECD countries

The banks, among other entities, are also obligated according to the implementation of OECD tax reporting standard [78] to clarify and report on all private, legal persons or their BOs, whose tax residence country is stated outside their reporting institution's local and inside any of the countries joined CRS/OECD tax reporting. To accomplish this, the KYC and CDD must be performed and verified through authority public and client's provided data confirmations.

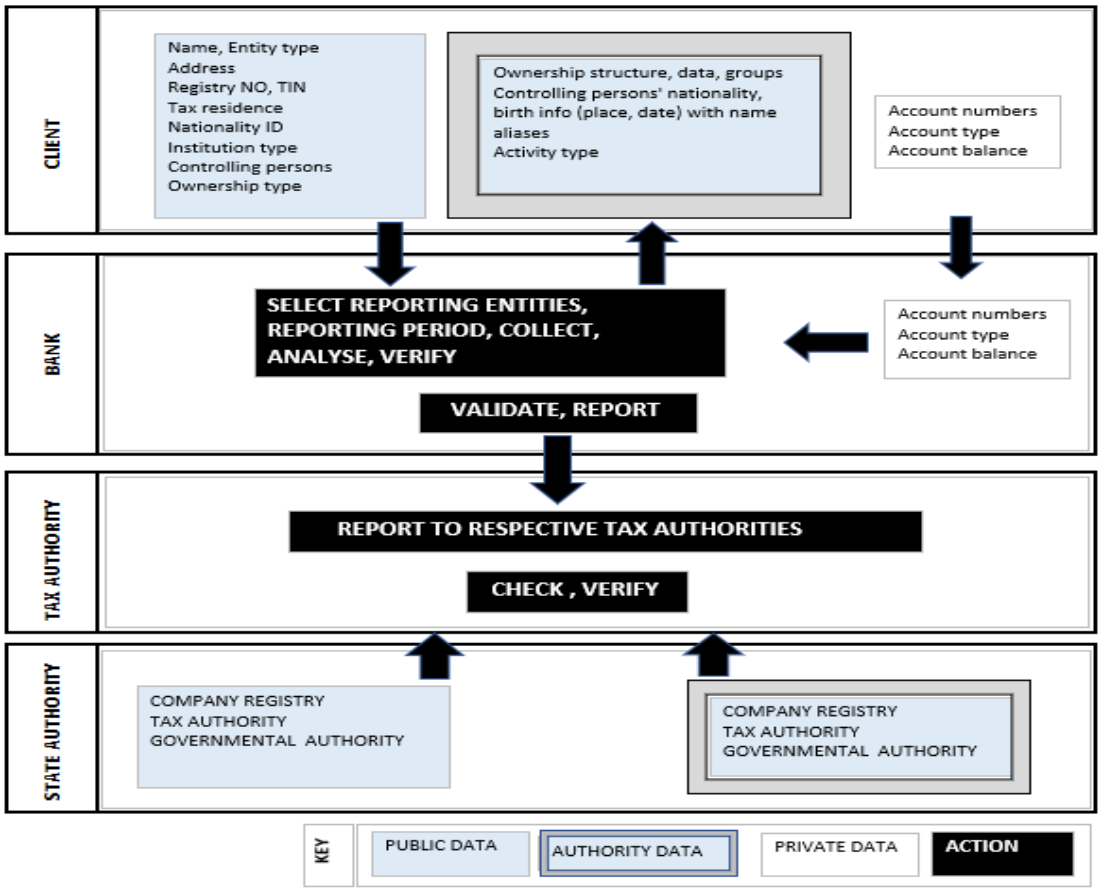

Figure 5. CRS external reporting dependencies

Precise information has to be given regarding the investment income, account balances, sales proceeds gathered according to the clients' entity and BO's data. Reporting has to be performed on year-end basis to local tax authority separately on every distinct country (separately client and BO if their tax residence is different) for the easiest data transfer by the latter to respective country's authority. The most common dependencies on this process are shown on the Figure 5.

4. Review of existing researches

In this chapter of existing researches on DLT, including its subcategories (blockchain, Hashgraph, DAG/Tangle), the applicable technology name is used what its founders of particular invention, service or consortium have stated as their ground technology. Nevertheless, the analyse itself has been executed keeping in mind broader DLT possibilities not to limit the solution only to one certain technology.

Existing projects in practice

The publicly revealed existing projects that started to explore exploiting DLT and especially blockchain in the banking industry were at first mostly related to payments and settlement (already in live) and trade finance (several currently in test phases) due to their complex and time-consuming execution. In the latter for instance IBM corporation has formed several blockchain projects - for instance the Batavia project [13] concluded by five banks, industry experts and clients. Batavia is planned as a new platform based on smart contracts, encoded to blockchain, planned to ease noticeably currently very laborious interactions in the trade finance area. Similar, blockchain with smart contracts, project but with the more partner banks with IBM we.trade (previously Digital Trade Chain Consortium) [14] is in test phase from February 2018.

Projects in search of ways to enhance the current real-time gross settlement using DLT are also run by numerous fintech companies, banks and regulators - like Bank of Japan and European Central Bank in the Stella report [18] and project Ubin [19] by the Monetary Authority of Singapore and the Association of Banks in Singapore. Corda permissioned need-to-know basis platform on DLT has introduced among trade finance (letter of credit deal executed by HSCB and Dutch ING [83]) and cross-border payments correspondingly application for AML and KYC purposes [50, 11]. Several authorities that advise European Commission on their area – as European Banking Authority and European Securities and Markets Authority have opened discussion papers on their approach of the financial technology (FinTech) on the usability of DLT and/or blockchain. The recipients of the mandatory reports - local FSA, Central Banks, Tax Authorities have been establishing secure platforms (sandboxes) where fintech and banking industry could securely find ways to efficient currently burdensome exchange of information. Extra initiative to find virtuous practise of innovative solutions comes from the financial technology companies to benefit under- or unserved areas and the regulatory technology (regtech) finds [22] ways to assist financial institutions to solve their present difficulties and achieve the target in less consuming, cost-effective, secure and efficient way.

Ripple [60], a permissionless distributed ledger operation likely to private ledger, as is regulated by validators [89], provides almost instant payments to participants with many assets (commodities, credits, loyalty points etc) in existing numerous currencies and Ripple own cryptocurrency (XRP) on DLT. Ripple is integrated with financial institutions' current systems. Transactions are cleared on the expense of customer provided deposit. It is stated that KYC and AML compliance is integrated into every transaction – by every gateway and Ripple promises to monitor payments (AML, fraud, sanctions) and report to regulators. The admittance to the monitoring processes and techniques is not accessible, but public information confirms Ripple's fine by FinCen on 2015 for not being compliant with AML/CTF monitoring obligations [82]. Open-source code Stellar which construction is federated Byzantine agreement (FBA) [61], uses above Ripple protocol, and is formed to introduce global network for monetary exchange. Stellar is decentralized, requires consensus and has therefore no single regulator. To ease the consensus handling, FBA introduced quorum slices and

slots, to which the participating nodes can diminish their requirement for asserting. As decentralized consensus is faced with ill-behaved, much of the power of the network is spent on proving the work which requires extensive amount expenses, time and other resources.

Other projects that focus on AML/CTF only are not accessible yet, due to the confidentiality reasons and no DLT projects were spotted on cross-border tax reporting. But their core issue, KYC, has been incorporated into many projects and touches in their features also AML/CTF issues.

Projects on KYC

Relevant projects in exactly the thesis area is KYC-Chain [15], built a blockchain and managed on DLT platform, for privates (using biometrics) and corporate customers to share their digital identity in a secure manner with financial institutions. Tangle [97], being a public ledger, descripted as "fundamentally different to blockchain" [98] has also declared that their setup of directed acyclic graph is projected to be used for ID wallet storing securely private data from health to identifications. Hedera Hashgraph, introduced innovative DLT has declared to offer AML and KYC compliance through their Opt-In Escrowed Identity system [100,25] allowing authority's approved identity to be shared with parties only the customer specifically so intends. Upon transactions from customers account with Hedera, the counterparty bank can verify customers ID only if customer allows access to it. These approaches would ease the control systems across borders and upon trusted parties identification this may ease the current process. Nevertheless, this requires a lot of unification settlements.

For global travellers the government of Canada has in collaboration with World Economic Forum and Accenture [47] built a prototype for travelers digital identity held on DLT hybrid ledger utilizing zero knowledge proof (ZKP) protocol, using Lewis's [41] introduced self-sovereign model which allows individual to be securely owner and sharer of his/her data however numerous contents of this (biometrics, bank details, passport number etc) are validated by issuing authorities. To accomplish this liberal approach the use of permissioned public ledger has been indicated as most suitable. The identity data saving solution and permission rights are currently open requiring more analyzes, whether to exploit DLT incorporated with blockchain, smart contracts or any other options. ZKP protocol is considered to bridge the privacy issues appearing in the DLT and blockchain as only the pointers to the sensitive information should be kept on DLT and not the actual data. This allows the participants to prove that the information, verified by authorities, is correct and trustful while the secured database saves the identity's signed parts of sensitive data and therefore the retention of private data would not be an impediment. Decentralized Identity Foundation [48], working together with Microsoft, Accenture and many others has used exactly zero-knowledge databases to implement global decentralized identity using blockchain ID. Positive is, that this form of digital ID, if proved to be solidly protected, could be used also in regular KYC process.

A report by the UK Government Chief Scientific Adviser [39, 74] values highly the possibility to enhance collaboration in different levels of assurance necessary for identification, cross-border business or proof of assets between the countries combining blockchain and public key infrastructure. Among others also Government Asia has revealed their plans to run KYC process onto DLT/blockchain [77]. The banks can access via shared KYC platform the data verified by trusted parties with customers permission only. Upon changes or regular updates, the verifications are shared via KYC platform and relevant bank stores applicable records and outcomes for their mandatory reporting. The latter tactics would aid the clients

and banks to operative verification process but will not relieve the excessive reporting requirements to the banks. At present such relevant standards and policies for secure information exchange exist for the police and would be beneficial for all if such experience and cooperation on secure and legal way could expand the interoperability in governmental /municipal authorities in and beyond state borders. Relevant method is exactly vital for redesigning the existing problems in stated processes especially in KYC and AML/CTF.

State Bank of India has started a DLT/blockchain security protocol based on KYC platform BankChain [80] with currently 35 consortium members and 10 projects under development to ease the bank compliance from trade finance to private and corporate KYC and identity handling. The set-up is private single node system where the owner sets the rules and provides access. This method would work for the redesign of processes if the protocol is decided by a consortium of regulators with possibility to change without damaging the existing system to achieve „cost reduction, while not losing the system control authority and initiative as is the goal of Korean Hana Bank in CDD enhancing project with collaboration with R3 CEV. As stated earlier, R3's Corda is the leading DLT platform, founded specially to serve financial institutions heightened needs from customer onboarding till termination and reporting. Numerous respectable consortium participants from central banks and regulators to financial institutions have also joined Corda to elaborate the exchange of securely trusted values and to grow out of "multiple generations of inefficient legacy technology" [94].

Similarly has acted global intermediary, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) providing the secure messaging system for its banking counterparties, starting their innovative programs from payments [20] to building a secure KYC platform [21], but this is not based on DLT nor blockchain and limited only for participating financial institutions. When considering the world wide digital identity scheme ID2020 [23] initiated by the United Nation, which objective is to give digital identity based on blockchain technology with the help of Microsoft and other organisations to those who have been not able to receive one in the first place, we can see that the field is growing and will quite soon be supported by more authorities. UN, being the trusted validator of given IDs, would able swift globalisation of identity approvals, permitting benefits of digitalisation and services to regions currently in lack.

Existing researches

DLT

Hearn [95] introduces Corda as peer-to-peer network utilising secure data managed coordination in decentralized global ledger with possibilities for secure semi-private access management necessary for banking industry and interoperability with future and current systems and ledgers. Admission to the network is authorised by selected participant(s), identification solved by public key tie to identity with possibility to elaborate similar names for avoiding mismatches, transactions could be verified by selected notaries or regulators (in a system or in selected regional legislative area) and transaction related data like timestamp, signings, attachments or identity, organised not into blocks, therefore revealed only on need to know basis. Assets information flow could be organised automatically, preselecting relevant information to required parties with the help of flow framework providing trackers [95,11]. All the data in the ledger is saved in the vault in opposite to blockchain wallets. Partakers data is shifted to its vault automatically from ledger and vault is able to manage preschedule dealings, fact/identity storing, or other smart contract- based actions required for smooth management. Smart contracts, in Corda named CorDapps, entail in encrypted way the necessary information for transaction execution, its triggers upon which occurrence the action

is automatically executed or not. Transactions history can be encrypted by Intel's technology named Software Guard Extensions to the extension that decryption is not possible even by Corda or holder of the transactions past ledger. The possibilities Corda provides with permissioned distributed ledger, would benefit aiding current difficulties if such an ecosystem for customer's identification, transfer and assets handling with accompanied fraud control and possibilities to interact to pre-agreed extent with similar ones globally is achieved without any secret back-doors.

Patel [49] has described the utility of Global Correspondent Banking Registry for banks to ease the problems related to cross-border transfers and of similar global, but country specific KYC register for clients. The latter collects besides identity proof data also all transactions of particular client world- wide and thus creating an all-inclusive view for the participating bank (if originates, mediates or receives particular payment) to access this data via Global Correspondent Banking Registry with country specific KYC registry and assess their willingness to conduct particular transaction beforehand to or with particular customer, compare this with other similar transactions data and conduct the payment even directly to beneficiary's bank, without using correspondent banks as current process requires. Same data would be available for regulators and FIU's to analyze. This approach is good in changing the current SAR reporting as on one-to-one model and allows broader view of the customer and their soundness of business and spend more time on analyses than verifying the collected data. But this would require unification of KYC collected data globally, solving the trust issues relating the information on registry with reputable 3rd parties and does not state the actual screening, analysis and reporting process relations with the regulators or banks. Same notification about unification and trustworthiness of data is pointed out by Staples *et al* [54].

The similar approach with permissioned DLT has been researched by Moyano and Ross [36]. They studied the possibilities of implementing centralized KYC process where financial institutions share their approval of verification of their client's KYC via permissioned DLT, held and maintained by the local regulator, among each other. Clearing was planned to be managed with smart contracts, privacy guaranteed by the verifying bank storing the clients' documents within its database sharing the cost of the verification anonymously and proportionately with other member banks. The system would be handled in two layers, one for customers and applications, the other - a fabric layer, for member banks. Firstly, upon customer's application a new account with public and private key would be created. Secondly, the analyse and verification is conducted by the bank with the help of customer's documents and shared public key, while exchanging the relevant documentation outside the distributed ledger. Thirdly, when the customer is validated or rejected, the verifying bank saves the decision with executed process and analysed documents in digitally signed smart contract kept both in bank's database and permissioned distributed ledger (fabric layer), but still attainable only to the customer and verifying bank. Fourthly, the verifying bank establishes smart contract with list of public keys future banking service provider of this customer could use to use the performed verification. A hash of all the documents the verifying bank produces are saved on the fabric layer, to provide more security for all involved parties. Authors "suggest that each bank uses a single, unique, one-payment-only account to interact with each customer" [36, 417] to provide secure interaction and privacy of participants. The above approach insures that a new bank who is interested in the particular verified customer is able to see how many public keys are in use and is able to receive its public key and benefit from the done verification only after it has compensated applicable proportional share of "the average price *m* conducting a core KYC verification process" [36, 417] via

cryptocurrency. This process promises to reduce costs, encourage competitors' collaboration, elevate the competition on particular market and cooperation with local authority. In the sense of this thesis the above Moyano and Ross [36] approach would improve customers' experience as it is one time only and gives the customer the control over permission (sharing keys) for sharing the access to the performed verification, benefit participating institutions in no minting as the verification can be shared only after proportional compensation. They also provide solutions to decentralize the KYC solution and not store analysed data on the fabric layer in case the regulator appears to be corrupt. As a weakness, this process does not consider that FATF's methodology [79] does not encourage relying on competitors' assessment, nor include risk rating and scoring of the customer and covers only the customer due diligence on onboarding (not mentioning future enhanced or any other regular due diligence necessary according to AML/CTF regulations). Also, if the verification rules and agreed criteria are not set and their compliance not controlled by the regulator and participating banks, the outcome of verification can be a chaos due to the differences in RBAs, business approach, value level and risk appetite of the different banks, especially in the current setup of blind trust and anonymous cooperation. The compensation costs could also differ from the above reasons, the multiple storage difficulties (upon further CDD) and expenses and the restriction to only use cryptocurrency for payments can also limit the actual use of this type of KYC optimization process.

Mills *et al* [102] have pointed out the potential of using DLT in settlement, including identity administration, storing and recording asset ownership together of executed transfers and controllers/regulators read-only access for regulatory reporting and compliance. This all is relevant also in current problem solving.

Yang [52] has studied several technologies available for security and privacy in DLT and ZKP is one of them diminishing the soundness errors to smallest amount. This requires storing sensitive data verification from 3rd party and respective public data and interaction orders visible between those to effectively execute the transaction or deal. Besides above, identification hiding techniques like ring signature founded in 2001 by Rivest, Shamir and Tauman [53] can be used to create transactions on public ledger without identifying the sender.

Subcategories of DLT

As payments solutions need to include in- or outside the used system also anti-money laundering tools, the business-to-business payments developed using DLT among the credit institutions is of great importance. As stated earlier, blockchain, being one possibility of creating distributed ledgers shareable for participants, not known to each other and therefore untrusted, on a network, should be also examined to find the best solution, nevertheless, many current projects and ventures fall under banking secrecy and are therefore in detail unapproachable yet. Buterin [96] has analysed possibilities of interoperation of different type of chains and their interaction strategy methods from parallel- and side chains with across triggers, arisen dependencies and validation possibilities. Easiest of which is through trusted and controlled notary positioned amid public and/or consortium chains. The option of relays, which gives different chains the same task, is not suitable in banking as verifications behind that could effortlessly made undistinguishable. If ledgers have similar consensus and agreed governance, the interoperability would be much more efficient and trustful as is necessary to solve stated problems regarding relevant screening, monitoring and reporting.

Yli-Huumo *et al* [101] researched blockchain technology, its limitations and possibilities to use it beyond cryptocurrency application as currently common. The potential range of usage

in different industries is wide. But the privacy and security, the most raised concerns of the decentralized environment and existing and unsolved problems with integrity, authentication, stolen privacy keys, vulnerability to obtained power majority overrun, could not suite as a whole (partially, yes) for solving current problems that necessitate security and privacy in many aspects.

Pisa and Juden [37] have searched the advantages, challenges and possible usage of blockchain technology in economy and refer to blockchain as an opportunity to generate distributed ledger on DLT as a protocol. Especially valuable regarding current topic reveals in their main aim to enhance the international cross-border payments, verification of identity and safeguarding the rights over assets. Their focus was to increase interoperability of current bank ledgers while spotting and minimizing illicit actions regarding money-laundering. They have set out an example scenario where all transfers are executed on the distributed ledger accompanied with customer's digital identification, so only the banks and participating customers could access this data and supervisors could have via digital dominant key to investigate these transactions according to subpoena. Authorities could also have the overlook of the anonymous flow of transactions to spot suspicious activities in real-time and analyse relevant data to detect trends of crime [37, 22]. Pisa and Juden have studied existing solutions of IDs in Estonia and India and pointed out that currently "internet lacks an identity layer" [37,24]. This example would be a good option for spotting trends in data protective environment, but it is preserving the existing analyse and monitoring in banks who are not able to see the bigger picture and assess own risks according to their experience and knowledge only after the payments are executed and funds left the bank.

Lewis on his blog Bits on Blocks [41] has introduced a simplified model of a self-sovereign identity which is created by the person to which the authorities provides further attestation, stored data is accessible over owner's phone or chip similar to credit card and protected with public and private keys. Pisa and Juden have elaborated this to the identification possibilities in an identity wallet [37, 25, figure V] with authorities assertations on a blockchain that could be enhancing the collaboration between the client and credit institutions. The governmental authorities approve name, gender, citizenship, marriage status of the owner of the wallet, employer his/her employment data and current bank his/her credit rating data. The owner of the wallet collects relevant accepted and approved data and shares this data only upon necessity with other banks with the aid of public and private keys. This should guarantee the privacy, traceability of relevant attributes and their records in the digital wallet. This approach could be very useful in public-private alliance ID2020 project to give digitalized identities to those private persons who due to various reasons are not provided by their birth or residence country valid identity. Houman Haddad [43], architect behind the Syrian refugees' identity restoration with eye iris scan, held in a permissioned part of Ethereum blockchain under the UN sub-program World Food Program, confirming existing identity via UN existing regular database. The challenges stated in this client- based method encounters is the upholding of this system, approving authorities, especially when wallet owner has international business and requires wallet for company use as well, participation and input part both cost, reliability and trust wise. If owner or/and authority uploads false approval, it would definitely require honest and trustworthy supervisor or regulator who would validate the righteousness.

Hybrid approach on identity related issues

The main issue in global approach that states use different and sometimes similar and overlapping identifiers. The only current global identifier available for companies is Legal Entity Identifier (LEI) [44], endorsed after 2008 crisis by the Financial Stability Board [46] and

ministerial forum of European Union and other 19 states over the world (G20) [45] to stabilize the economy over the world, use LEI to trace and report corporates and their securities trading. LEI 20-digit number incorporates also data about the corporates identification, group's ownership structure and therefore comes of a benefit during the identification process of KYC. R3 DLT project "is considering using the LEI as the primary identifier embedded in its digital certificates" [44,24]. As the LEI's issuance is costly for the customer, it is not available for privates and is valid only with certain terms, their usage as universal global identifier is currently not the case.

Stemming from LEI, the securities transactions, that require instant reporting of transactions are forming the majority of in-live numerous DLT and blockchain platforms. Peters *et al* [58] researched the DLT usability in financial instrument and trade transaction transparency and reporting. They point out advantages of permissioned purpose-built ledgers (Hyperledger, Ripple, etc) was their compatibility with current systems handling off-chain assets, achievable collaboration and consensus in amending rules, legal accountability and scalability. LEI, as required for financial transactions, is key in reporting. Hybrid-blockchain held by full access right authority or consortium of financial institutions (access and amend their clients data upon changes) is suggested for company's identification. Personal data would be secured in encrypted way on-chain accompanied with unique ID. If decentralized ledger is used, the transactions would be kept on a private chain, to which the authority's access would be in predefined readable format. Peters *et al* approach, nevertheless meant for financial transactions reporting is valuable also in this research reporting to tax authority.

Finextra blog [42] has covered interaction and existing data transfer possibilities of non-DLT systems to DLT solutions, (as for instance) payments and securities settlement RIPPLE, onto DLT. This would require international legal entity identifier so all trusted participants of permissioned /public / hybrid blockchain or ledger could amend necessary data and others could reach that data. Other relevant data like address, PEP, BO, tax residency, account details could also be stored in the wallet and banks, when assess alerts of money-laundering, could evaluate instantly the received data and share the details of such transactions to globally participating banks. This approach would be very useful in catching the actual transactions of money-laundering or terrorist financing, but as this does not alter the alert creating and assessing approach, the illicit funds would be long gone from wallet as the monitoring and SAR reporting takes time. Therefore, if regulators and FIU's would be connected to the system or have access to it, they would receive the information in early stage and seize the funds on the spot. This would require a lot of input from regulators, would revert their current post-action investigations of suspicious deals to possibilities to be able to pinpoint issues on spot and be viewing and analyzing possible trends in illicit activities. Similarly to above wallets, Corda customer vault could have the same possibility without private data being spread across all participants. Interoperability of those approaches would broaden the possibilities in identity matching with transactions and enhance the spotting of illicit attempts and transactions.

Compliance options

Stemming from raising compliance issues, Woodsome and Ramachandran [84] gathered researches of using DLT/blockchain in solving the money-laundering difficulties banks face. Referring to possibilities of structuring data on DLT, the term blockchain is stated as the method of data storage "such that the ledger retains the entire history of data modifications," [84, 48] which is accepted and stored by partakers in time-stamped linked blocks. Machine learning together with available big data analyses is encouraged for efficient risk

management and interaction between the banks, clients and FIUs in KYC and AML matters. Regulators and FIUs are reminded to lift some burden off over-regulated banks to limit the likelihood of shifting transactions services into less-regulated networks. This trend enlarges with technology development and banks stringier actions to mitigate risks and is one of the reasons why regulators should look forward towards risk shifting technology possibilities.

Stark [51] has researched the possibilities using R3 Corda DLT applications for regulatory compliance in reporting obligatory information on interest swap transactions by building the reporting into the system and allowing, by the permission of the bank stated in specific Corda application CorApp, the regulators nodes to receive access to the relevant agreement, with verification by the designated notary node, directly after its conclusion. This method easies alterations upon changes in regulative demands and rules, allows actually more information sharing to regulators with lower costs, diminishes current data sharing that regulators already should have access to and permits better regulatory confidence as the built-in conditional approach will not allow performance of any transactions unless all regulatory pre-conditions are met correctly. Regretfully, this scheme does not diminish monitoring analysis compulsory to banks.

Besides reporting, the demands from authorities regarding data protection, rectifications and expired data retention have encouraged specialist to discuss on this matter due to DLT's known immutability and complications accompanying with necessary amendments to incorrect data. KWORI [55], Vranken [56] and Bacon [57,51] have pointed out the possibilities to comply data protection in DLT. The banking law and DLT protocols are not yet very efficient for permissionless ledger, which upon the retention or any change could be executed with collaboration of almost all the parties or their assigned group members. Therefore, in current state the data requiring retention, should be stored on smart contracts (not visible to non-parties) without losing the scalability. Kosba *et al* [40] studied the version of increasing privacy, diminishing the data saved on blockchain with help of smart contracts in a protocol Hawk that requires ZKP (in the contrary to regular blockchain) and contains of two portions – on-chain public and contractual private (for sensitive data) – in the decentralized cryptocurrency system overlooked by marginally trusted manager or trusted computing hardware. Hawk framework usage was shown among other possibilities also on swap instruments where the manager would be stock-exchange and to guarantee the fairness in case one party cheats, the public collateral deposit. Analysed ways of leveraging different cases of corruption and unfairness could be used in future global networks for protecting parties active in public ledgers and also against counterparties to the contractual private ledger.

Taxation solution on blockchain for personal taxi service like Uber in Denmark was studied by Warnez [59] with proposal to solve payment and correlated instant taxation via smart contracts using Danish Crown equivalent tokens swapped by the local central bank. Warnez prefers the local Tax Authority to govern the permissioned ledger as taxation is considered legal obligation and therefore the data protection could be handled according to the law. The Certificate Authority certificates in permissioned ledger allows the Tax Authority to correct default or wrongly inputted transactions on the chain more easily. Nevertheless, the monetary problems, similar approach can be used if taxation verification necessary in some countries also locally.

5. Redesign of current processes

5.1 Overall management

As derived from current knowledge and limited possibilities, lacking protocols and standards for DLT, the research, experience and tests of other regulators and banks lead to the solution that the most efficient solution to all above raised problems would be using private/permissioned distributed ledger network available for all applicable stakeholders within a region or state/country, with ZKP [52], allowing timestamped and restricted access smart contracts. Also, the possibility to read-only relevant public data on private ledger available to all according to the law, is a must. The protocol, as mainstay for the system, should be managed and planned by the state, which grounds could be used developed with the aid of specialists or selecting among existing protocols, supporting above tactic, such as for instance Corda. To interact with the different stakeholders and ledgers, the application layer (here also depending on the activity named also verification and control layer) would be joined with numerous other mutually trusted pertinent systems (FIU cooperation, regulators, users). The utmost different approach from current one is that due to the knowledge, cooperation and larger scope available for states, the current bank's role as a gatekeeper in AML/CTF would, in re-designed process with the abilities of advanced technology and stemming state's risks at stake, be shifted to the state's authority. State, in the form of super user would handle together with its relevant entities (registries, FSA, FIU, etc) region's access granting and user management depending on the partakers license and supervisory, identity verification (KYC, CDD) of their citizens and local companies with their UBO/BO and automatic pre-transaction analyze. For this, the permissioned DLT would be in conformity with current banking security regulations and trust issue, as administration rights and responsibility over data validation are more visible and countable in the contrary to the public distributed ledger where "no legal entity owns or controls the ledger" [30, 12]. Where relevant and scalable, blockchain could be used with interoperability possibilities for control and data retrieval from other type of ledgers.

The private and corporate customers and their UBO/BOs data, to the extent mandatory by the law, would be required to keep available to public and therefore visible from the public part of the private distributed ledger sustained by the state or state appointed controller. Legal obligations stemming from the law are of the public interest and therefore in this case the data protection regarding retention will be not that stringent and therefore could be managed with private blockchain. If not, this requires with future changes in legal demands the storage of chronological history and hence such data should be also stored with timestamping and approved by BO, company and respective authority. The private data as agreements and counterparties verifications would be kept on private smart contracts, which content can be changed when necessary. To the latter information the client with the permission of its counterparty would allow access to the bank directly and relevant local FIU (directly or via control layer) upon establishing the business relations. The customer's and bank's part of the public DLT ledger would be managed with the relevant (public) code with public and private key match that allows all parties access for verifications and a specific support from the managing state would be provided for participants.

The state can also use the existing ledgers parallel to DLT ledgers and run its data all through control/verification layer, whichever is currently necessary. In enhancing current approach of KYC, AML/CTF, CRS and FATCA reporting besides banking institutions also other participants future rights and obligations are taken in account. The latter are for clients the data protection related retention or amend of data, for states/regions the following of the

FATF imposed standards (recommendations, methods, procedures) [72] and related upcoming requirements of the European 5th directive of Anti-Money Laundering [71] of establishing local centralised bank account (similar to real estate) and UBO registries, for FIUs broadened interaction and exchange of information and for banks the enhanced checks on transfers to countries not following sanctions. These redesigned processes necessitate non-corrupt supervisor access, control and prompt interference mechanisms over possibly shady or tendency to dishonesty states and/or their participating institutions/authorities.

The future secure interactions of centralized and counter trusted public ledger would also aid diminishing possibility of corruption in places the corruption of state authorities cannot be avoided. For instance, the global projects like ID2020 (for privates and their micro enterprises) the identity verifier would take, at least partly, the role typically handled by state (verification, managing the registry), allowing legal business and funds, via interactions with agreeing authorities' private ledgers, into places presently constrained for political or governing reasons.

5.2 Re-designed KYC reporting

The planned dependencies of the new KYC procedure are outlaid on Figure 6. Firstly, the data appearance or change necessary according to the law is governed.

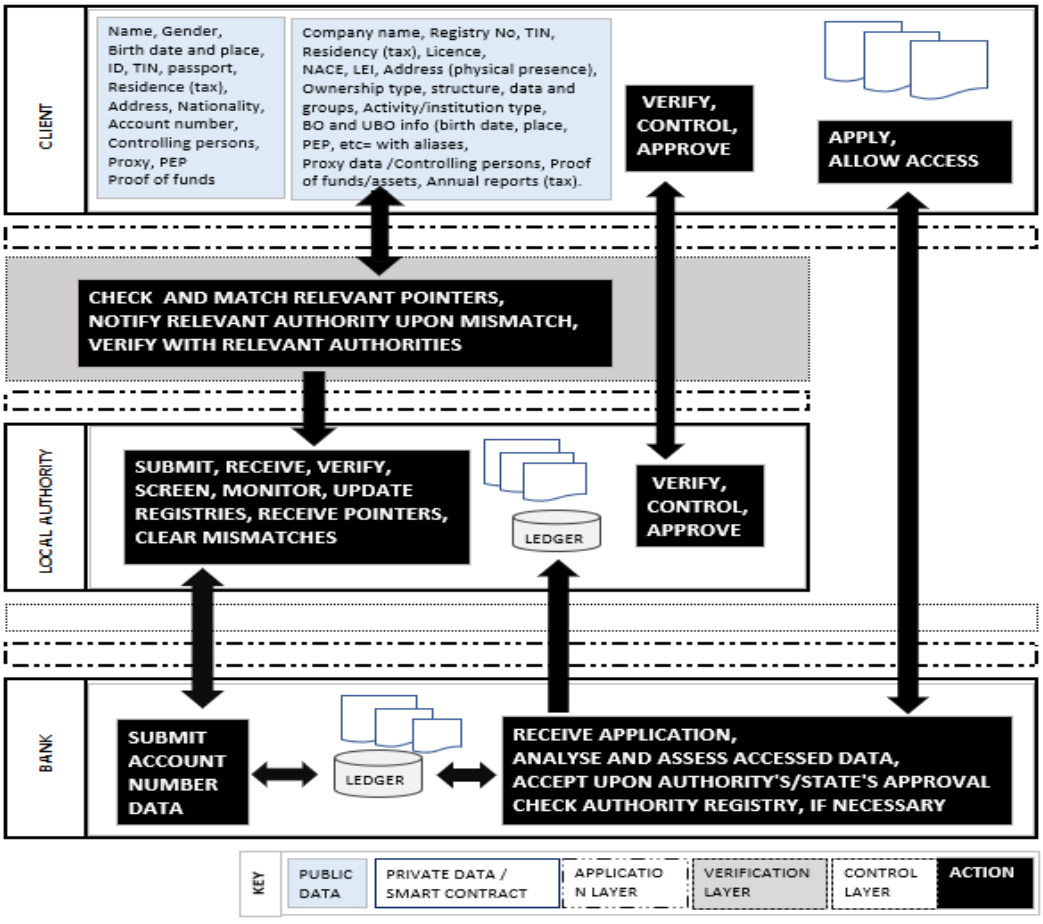

Figure 6. KYC dependencies with DLT

Each private or corporate customer (including banks, but in more elaborate and reticent way) has different type of legally obligated data stowed on the register, of which legally required and verified content is seeable to all. Entering such data is triggered by numerous acts, from birth to establishing or selling a company. Triggering event related data is entered the ledger

by either party, depending on the event. The customer accesses the state managed ledger via application layer identifying itself with applicable public and private codes. Subsequently the verification layer collects and analyses existing data on the customer in the state different authorities ledgers and verifies this data with relevant authorities joined separately with the ledger (for example tax authority, state managed license issuers, FSA, FIU, police, locally approved necessary watchlists) or contracting parties (such as LEI issuers, bank, notary) via the verification layer with the state and notifies both customer and relevant participants of found and unresolved mismatches automatically. The customer verification of data is considered any term of self-certification required according to the law. For minors the verification control is done by parents or state proxy, if so sated in the local law. The matching alert data received via watchlists about the privates, corporates or their business area (target business, proliferation) or agenda, analyzed by the state relevant authorities prior to the final approval and outcome with findings kept on the private part of the state ledger accessible according to the relevant contracts to the international FIUs, courts and other pertinent institutions. Comparable analyses and information should be obtainable for other FIUs during the FATF initiated cooperation.

The more number of participating stakeholders are connected to the verification layer or state managed ledger directly, the better the quality of the public data on the customer. After the mismatches are cleared with the help and proof of authorities and customer, only the necessary data of the customer is made public (all enterers possess reading rights). The customer carries the obligation to keep its data updated at least one a year and inform the state authority when the trigger requesting a change is on the customer's side during that period. The verification layer informs automatically customer of upcoming yearly update or of any authority raised alteration on its data on the public ledger and the customer is required to either accept or reject the above change informing via application layer the state authority. The latter is reliable of checking, storing and publishing, if required, this verified data correctly and on time. Both, the customer, and state have identical verified data, all other data at state's disposal may not need verification from the customer. After the customer applies for the bank account and approves the bank's access to its public and applicable private data existing only on smart contracts, the bank can assess the suitability of the customer and accompanying risks. If the data of the potential customer is not approved by relevant public authority, the bank is allowed to access particular customer's banking related data via application layer from the local authority for clarification. The latter is necessary also if the customer and bank do not belong to the same region/state. All not public data between the authority, client and/or the bank are shared on the smart contract accessible only to parties with such permission and stored on parties' ledgers. The control layer in KYC process is linked also to the AML/CTF control layer screening the watchlists and spotting the fraud on Figure 7, to avoid criminals using the state's structures.

This proposed approach would benefit all the stakeholders within the joined states and regions to possess always the updated unified KYC data in timesaving and data protective manner and to help avoid global criminals slide-in and legalize their fraudulent acts and funds victimizing and damaging the state's economy. The more regions or states, directly or through trusted 3rd parties, are united in this consortium, the more scalable and advantageous this approach is. Regular yearly updates would also serve the necessary CDD requirement. EDD, necessary to perform on high-risk customers, could be done even more frequently and to manage it in accordance with the FATF recommendations, the state/region should oblige and notify via verification layer the riskier customers (according to person related, business, geographic, jurisdictional or technical compliance [73] area) to update their data once per half-year. Besides above this process allows relevant authority to receive

automatic knowledge on declined customer relations, terminated accounts and its reasoning, currently handled under regulatory reporting on consumer protection, credits and liquidity. With more specific and correspondingly private data, this KYC approach could be also used for fintech payment service providers (PSP), commercial banks and their due diligence, currently implemented together with payment system by Ripple [68].

5.3 Re-designed AML/CTF reporting

According to the deliberately not revealed and often guessed statistic on the actual number of funds being laundered, used for terrorism or financing (proliferation) weapons of mass destruction, and how many of these fraudulent acts and funds are actually being prosecuted and seized, is ambiguous. Consequently, the idea that needs to be addressed is by what means to prevent these delinquencies in the first place, prior the funds have been transferred, as this would avert the possibility that the region is used for illegitimate financial activities. The below tactic, shown of Figure 7, enacts in the broadening scope of executing payments the similar potential of regionally unified pre-emptive actions and countermeasures as is accomplished in the commonly acknowledged medical prescription delivery process. Hence the data, besides public KYC data, shared in this process necessitates more restraint line guaranteed by the permissioned distributed ledger.

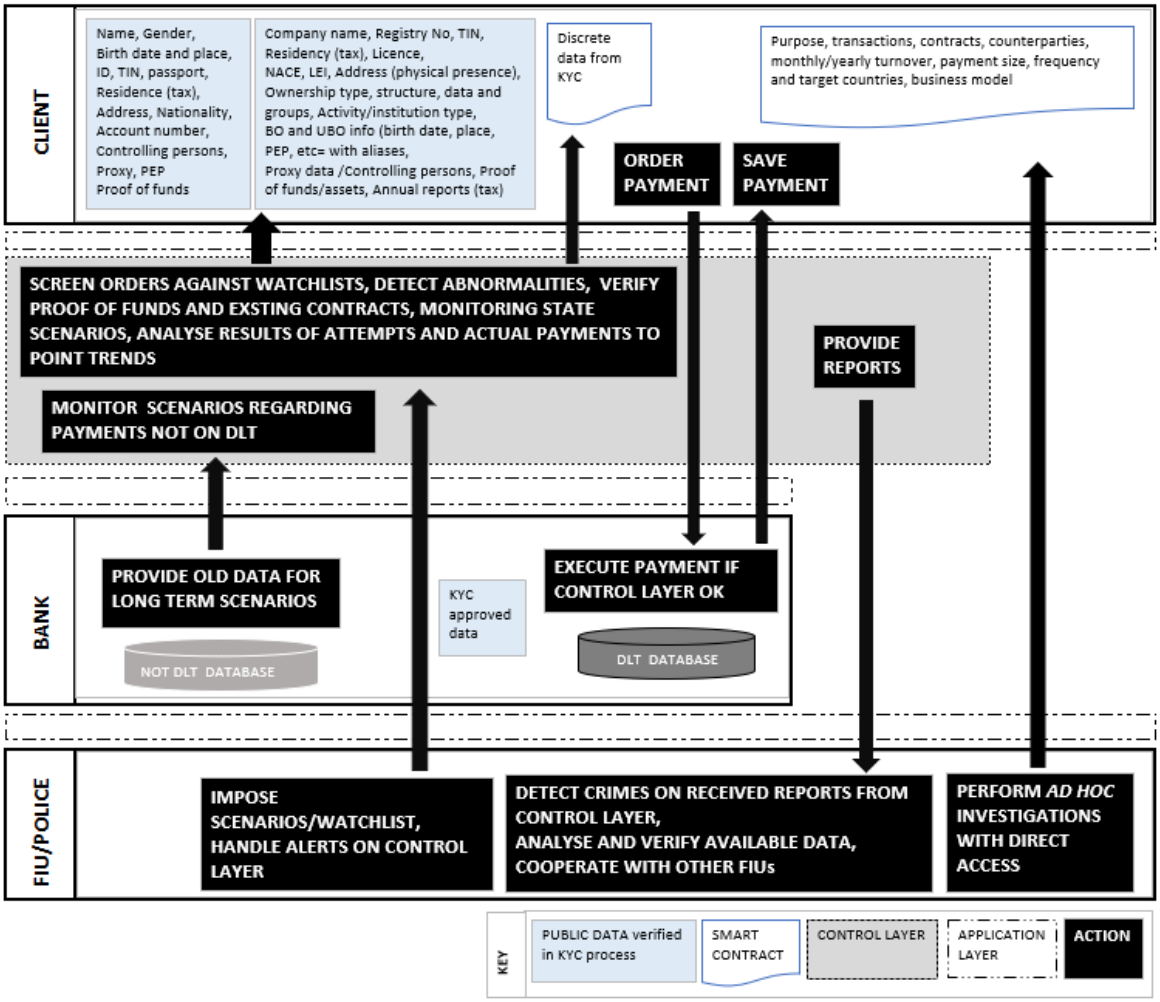

Figure 7. AML/CTF external reporting dependencies with DLT

Firstly, the state (ideally together with their colleague authorities and regulators from other countries) managing the ledger, through its relevant authority (usually consortium of

FIUs/police with possibility to localize and specify the requirements) imposes the scenarios, watchlists and relevant data onto the control layer. For each bank the control level is adaptable stemming from their risk appetite agreed prior with the applicable authorities. Secondly, the customer submits the payment order, triggered by the smart contract (or any other means, if applicable) indicating that the payable service is provided and received, and proof of funds available in the smart contract, through the control layer to the bank/PSP. If the customer has changed the data in the smart contract, the control layer can automatically check it upon the customer's payment order. The customer's order is made via application layer and it passes the control layer, where the state authority automatically screens, monitors, swiftly analyses and releases lawful funds already before the payment order reaches the bank for execution. If the customer orders the bank or PSP to initiate the payment, the service provider can initiate the order for the customer and keep the above process. Same approach will apply to incoming payments. The outcome of the latter is automatic analyse of lawfulness, assessed risk and mitigation suggestions of the particular transaction, its content, parties, and assets taking into account risks regarding customer's behaviour and the sanctions imposed on the receivable country/region, recipient or customer personal or business area. Thirdly, the bank obtains order via control layer together with a risk evaluation notice (outcome of the automatic analyse) in the form of smart contract not accessible to customer and weighs these risks automatically with alerts upon non-conformity with bank's risk appetize, internal instructions, controls and either via the application layer executes the transfer or rejects it. If the payment is executed despite of state's restrictive notice, the FIU automatically receives such alert together with all necessary documents and proof. If bank decides, on the proven risk grounds to blocks the funds or account, the control layer is notified automatically. The control layer content with transaction data with applicable smart contracts is accessible only to the state authority and to their controllers. In this way the control layer is a source of data with payment orders via banks or any other kind of current or future service providers whether executed or not together with attempts of possibly fraudulent transfers to pinpoint or foresee the pattern. This tactic, although probably slowing down the instant payments could limit the control being executed only once (if all parties are joined), would able to point and seize the illegal funds prior their transfer, stop usage of accounts used for money-laundering, terrorist financing or proliferation and save funds for detecting illegal funds post-action as currently.

To guarantee the secrecy necessary for AML/CTF related investigations, the customer, by giving the access for authorities and applicable bank/PSP into its smart contracts, should not see exactly which authority has accessed the data. For the bank/PSP or FIU this proof of control is demanded for the audit trail. With new tactics, FATF's, through stated methodology for technical compliance [79], highest goal to protect the economy overall and not to limit only with financial institutions, would be reachable to much higher level than currently where the state is as money-laundering proof as its weakest capability bank.

Privacy protection in regions where the AML/CTF controls are not inserted into the local law or the supervisors or regulatory are not considered trustworthy, the AML process could be also solved as proposed by the Finextra [42] that allows the customers evaluated by the respected regulatory or organisation (United Nations) to access financial transfers by storing all executed transactions, contracts and funds proof data onto its own digital wallet, so all permissioned institutions, could access and asses the customer according to that. This case entails the risk of the customer being able to hide/delete/not insert all transaction data into the wallet.

The same risk, that some corrupt FIU may taint or manipulate data or legalise illegal data on the control layer, is also possible, but to guarantee the required line of defences in compliance and to avoid overruling or misuse of power and leakage of methods or investigated data in AML/CTF reporting, the local FSAs, controlled by their cross-border supervisor authorities, should have access to FIU's and PSP/bank's transaction-related analyse proof and existing procedures as visible in the Figure 8. In the light of 5th AML Directive requirement for cross-border cooperation, this approach would enable it for FIUs, the regulatory and supervisory level and have admittance to pertinent data.

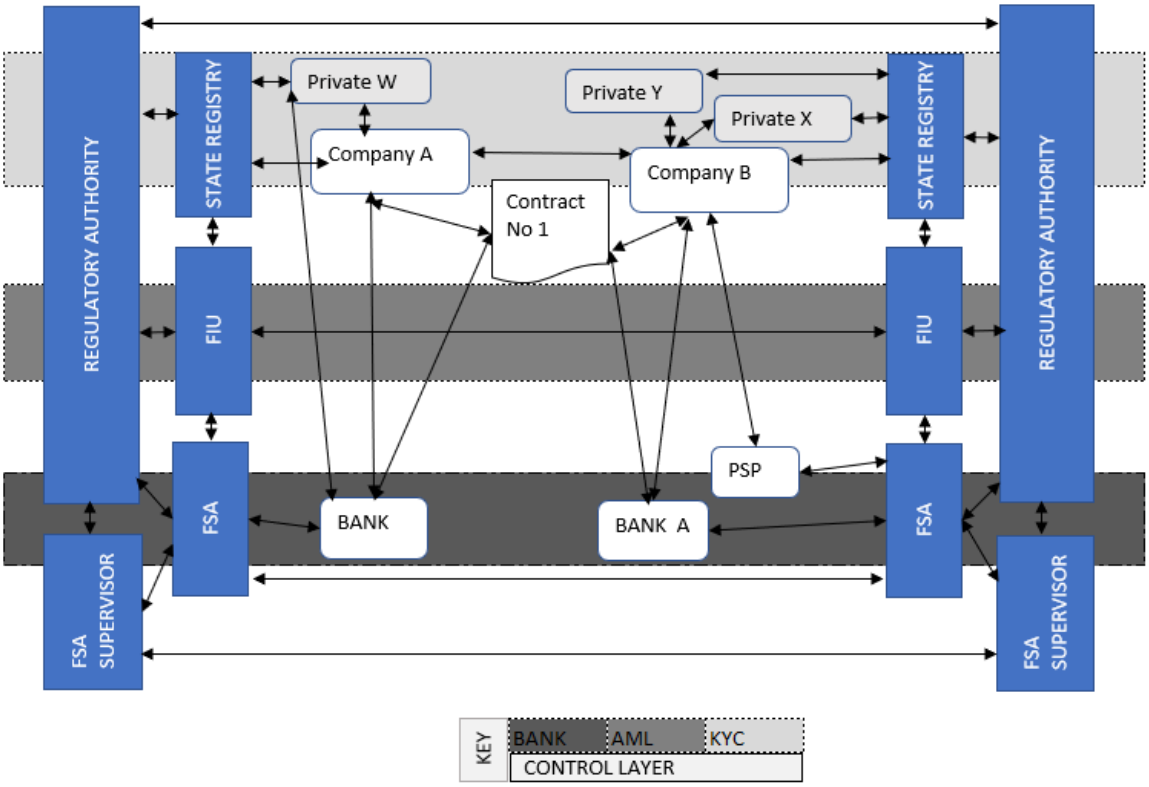

Figure 8. AML/CTF control layers and participants interaction dependencies among different regulatory areas with DLT

With the technology offering more easier possibilities, the future of the payment services would most likely shift to specialised service providers or even direct peer-to-peer payments outside banks and this system would allow integrating all participants and their payments as well already from their beginning would also be transferred via control layer.

5.4 FATCA to be

FATCA tax reporting for financial institutions was founded as a mean to discover and control over the U.S. customers hiding their taxable income worldwide behind the complicated net of assets and companies with danger to withhold 30% taxes on every not-joined financial institution' U.S. originated payments.

In redesigned process on Figure 9, the control layer, held by the state as in the AML/CTF redesign Figure 7 and verification layer in KYC redesign Figure 6, detects besides watchlists incentives also variables related to US (pointers) - data on US indicia on the customer and their BOs from KYC process and US origin payments not verified in the smart contract by the valid IRS forms. This allows to point customers with US taxable funds and verify the account balance, type and status from the smart contract held by the bank on that customer.

The same smart contracts would be held by the customer for the further tax purposes and proof or permissioned access by tax advisor, accountant or previous or new tax residence tax authority. Similar is held if the US indicia is being dropped and customer or its funds are no longer reportable/with-holdable according to FATCA.

Tax authority accesses via application layer the above public data and other tax related data on the customer within its jurisdiction upon provided access to pertinent smart contracts by the customer or according to the law from bank and concludes and transfers the report to IRS automatically. Bank's internal database should notify automatically local tax authority via application layer of any U.S. indicia not incorporated to KYC process (phone, e-mail) found during the customer relationship, so the tax authority can control if this info should lead to withholding of the funds. Upon such outcome the tax authority informs automatically via application layer all banks the customer and companies where s/he is BO have the account with to the conditions (every or just U.S. receivables, tax rate) of withholding and transferring the tax.

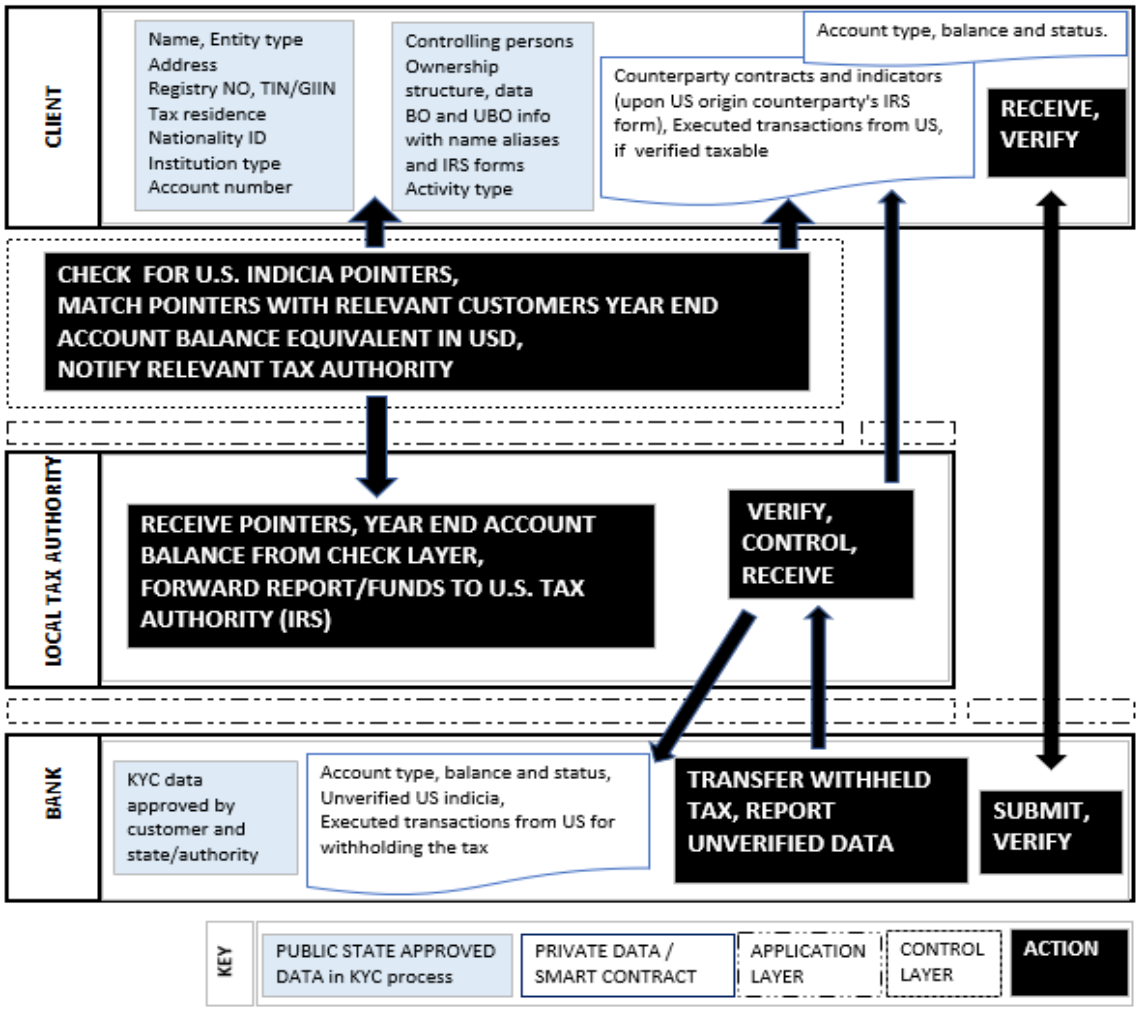

Figure 9. FATCA external reporting dependencies with DLT

This approach would elevate the global interaction in tax collecting and aid handling with discrepancies accompanied with double-triple taxation. Tax authority executes this directly within its jurisdiction and to relevant tax authorities for pass-on to banks they control, according to their cooperation and information change channels more swiftly than currently. For such customers an applicable smart contract on their payments originated from U.S. or relevant interests, dividends or other taxable funds, would be held in a smart contract in the

same way as the one kept on the above stated account status. Similar process would be initiated and relevant banks informed if any state authority directly or via tax authority investigates that the customer is no longer reportable to IRS due to any reason. Same release could be given directly to all relevant tax authorities by IRS if the latter accesses customer's smart contract and approves the customer bank's approval to the content regarding customer type, account balance and status.

Above tactics on Figure 9 would be effectual for so called new customers (from 2014). In case the U.S. indicia appears through any means on the pre- 2014 customers, the similar approach as above could be imposed regardless of the threshold and increase the tax receivables of U.S. Currently only those pre-2014 accounts that on certain year end raise above stated threshold should be controlled for U.S. indicia and reported.

Renewed process shifts the gatekeeper role to tax authorities, automates the control and diminishes the presenting and transferring of false or multiple reports from different countries and banks. This allows closer cross-border cooperation among different tax authorities to pinpoint, analyse and withhold the funds of exactly relevant persons avoiding taxes not only related to U.S., but also other countries as shown below in CRS process restructure.

5.5 CRS to be

Likewise FATCA, the tax CRS/OECD reporting bears in mind the same purpose – more accurate tax payments and pinpointing the tax evaders, but without tax collective requirement and punitive charges for non-followers.

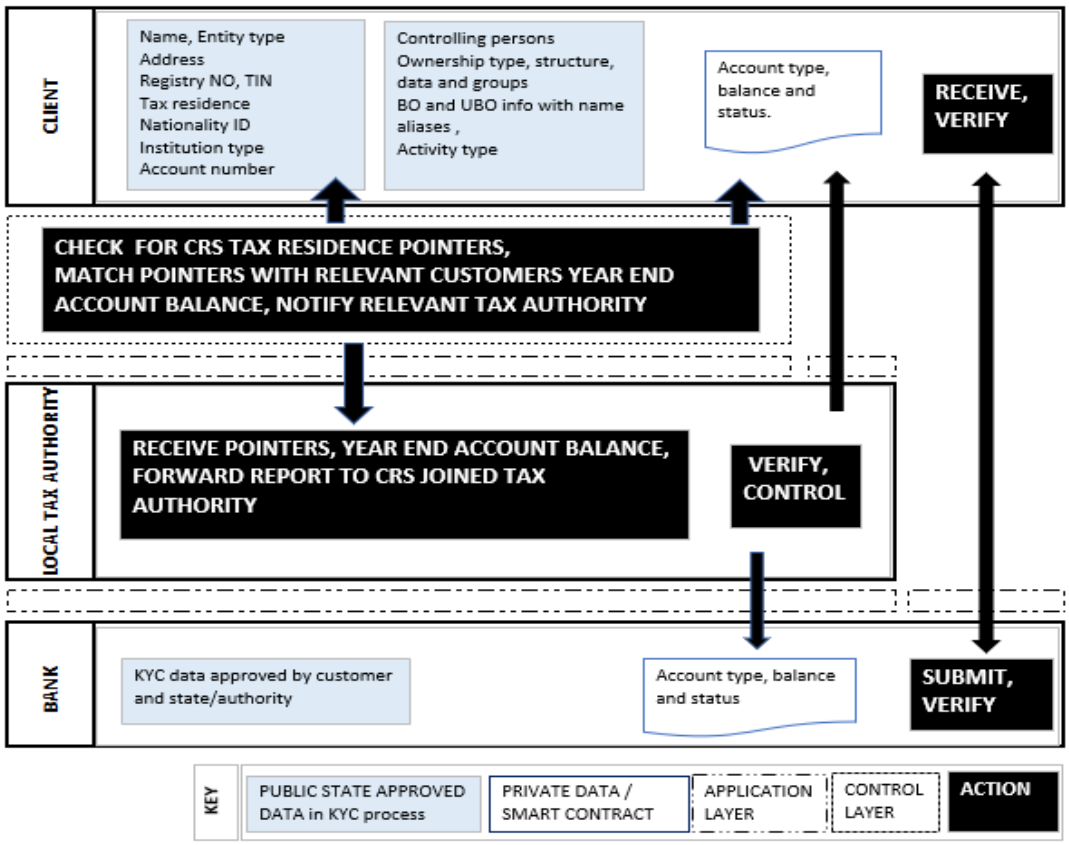

Figure 10. CRS external reporting dependencies with DLT

CRS depends on financial institutions detecting reportable accounts, collecting, verifying and reporting the data to local tax authority for analyze and transfer to applicable country's

authority. Currently the bank can trust the client to some extent and accept their provided data on their confirmations on residency, BOs and their data.

In this renewed approach on Figure 10, the states through its respective authorities, take the matter in their hands, verify, similarly to KYC (Figure 6) and AML/CTF (Figure 7) renewed reporting through control layer all relevant customer, relevant smart contracts and BOs data at their disposal, limiting current fabrications and abuse of the state economy. Unlike the banks, the state has more information on what services their citizens/companies use to pin-point their genuine residency and whether this is actually their citizen who is taxable. State can identify and prevent also other ways of masking the true residency with much more ease than banks currently and adapt swiftly if the thresholds for BO's are altered.

Similar method can be utilised in other regulatory reporting like bank's Comprehensive Capital Analysis and Review (CCAR). This could be unified with FATCA for the more approachable system worldwide, especially taking account how costly the collection and reporting is, the new approach could join more countries with lesser demands. This approach abeles adjusting the current standard to more modern and changing world and aid to combat tax evasion to the better extent. Applicable also to insurance companies, investment schemes, to prevent pension and other social benefit double payouts depending on the residence of the customer and its investments, suffocate the tax heaven's approaches of masking identity of customers, finding taxpayers falling using the loopholes (trust, holdings) allowing avoiding the taxation of investments into cryptocurrency in tax residence country where this is not allowed.

Therefore, the most efficient way to utilize this reporting goal is to shift as in previous processes, the first verification proof to the interaction of customer and their residency state authorities and their cross-border cooperation. This enlarges the states' knowledge of their citizens, their businesses, the non-residents living or engaging in commercial activities, possibilities for real-data analyses for enhancing the business environment within the region and of course tax receivables when similar approach is used towards local privates and companies for tax control.

6. Discussion

The root for this thesis is grounded in the actual need to comfort vastly growing mandatory reporting's impact on banks who provide informational aid, an origin from the past limited possibilities of technology, to the police, tax and state other investigating authorities. The aim of current reporting to states, achieved due to the availability of transactions info within and better means to influence the client to provide necessary information to banks, is helping to check cross-border taxpayers reported dues and spot criminal financial transfers.

To accomplish the latter, high quality data is required from the customer by every bank separately. Only some new requirements allow banks simply to rely on client's confirmation, while the rest of clients' credentials and activities necessitates continuous verification from different parties and databases, analyse and assessment of possible risks accompanied with servicing each customer to mitigate and keep residue risk on the level acceptable to bank and its regulating state(s). The outcome of this process is apparently diverse for every bank and their reports, as accessible data on client and its transfers as a whole, is limited. The availability of unified verified data would permit assessments being more in line with the customer's actual risk level in particular state/region, be relieving for the customer in communication and document exchange and benefit the state in knowing their citizens, businesses and organising safer and secure financial environment.

Possibilities of DLT and its sub-categories

Hence the available potentials and impediments of DLT and its subcategories, to overcome the existing issues with communication, verification, analyse and reporting between persons, institutions and relevant ledgers, were studied. The analysed possibilities of DLT, in whatever future or existing form, blockchain, Hashgraph, Tangle or other public or peer-to peer private ledgers efficient for transactions performing, is fairly novel, technical proficiency and actual steps particularly in KYC, AML/CTF and tax reporting area is rare and willingness to execute could be tainted due to problems with bitcoin, trust and cost. Nonetheless, many introduced standardisation initiatives [92; 93], prodigious examples in consortiums of authorities, technology companies and banks (Ubin, Corda), securities payments and trade finance, should encourage to study DLT's potentials to improve and minimise current risks in tax evasion and criminal activities states face through banks. DLT strengths – handling verification through public key cryptography, approving private and alterable data on smart contract with timestamps and fingerprinting hash, organising own governance protocols and standards for permissioned ledgers, attaching current ledgers with DLT ledgers, using, storing and sharing that in any format efficiently with ZKP protocols, automatic controls, easy access via different purpose layers, resilience for malicious partakers in contrary with public blockchain approach, interaction with other/controlling regulators and ledgers – could aid to reach the goal of consortium of non-corrupt jurisdictions and regulators to join knowledge and forces as gatekeepers in combating the related crime on spot. The latter is possible when a trustworthy digital infrastructure with built-in control mechanism for regulators' is created for local and global interactions as shown in Figure 8.

Reasoning

With technology driven inventions and related global services rise, current control or verifications methods will not serve us well in the near future. The state's strength to combat money-laundering, evaluated continuously by FATF, is as durable as its weakest bank's capabilities allow. As the technology develops, new payment possibilities emerge, the states face broadened impacts of money-laundering and tax evasion, hence new means to control their region must be advanced. At first, when analysing, would the possibilities of DLT

relive compliance problems in generating and presenting the required reports, the idea was not automation of analysing and presenting the reports as is also possible now but giving the state's particular authority the access to certain data directly after the state, according to FATF, distinguishes all accounts its every citizen or company has. But stemming from the data circle, which begins (ID, opening company) and ends (SAR, prosecution) with the state authority, but requires banks analyse in between, led to the idea to utilise the DLT features of interoperability with different types of ledgers, secure vaults, trust, access and performance control, smart contracts triggering activities, not depending on not-known participants, and allow shifting fraud controls back to the authorities.

Redesigned approach

As the current banking system requires protection of its secrecy, the most efficient approach to all problems at stake would be using private distributed ledger network available for all applicable stakeholders within a region or state/country, with ZKP [52], allowing timestamped and restricted access smart contracts. The ecosystems protocol, as mainstay, should be managed (founding, content, maintaining, access control) by the state supporting local difference taking in mind the interoperability necessities with numerous types of local and cross-border ledgers and partakers, if willing, using existing protocols as for instance Corda.

New ecosystem should firstly utilise the existing information, on private and corporate customers in the different local authorities' current databases, structural incorporation to the state managed permissioned ledger. This data, verified by the state securely, privately (with public key or any future cryptography) and directly with particular customer joining this ledger via application, requires approved protocol for its future use, access and release as shown on Figure 6. Legally public information should stay available in a regular updated form (on blockchain) to all as is currently in most countries, but in a verified form, so all banks, PSPs and other companies requiring authentication and know-their-customers (unified KYC), could rely on that and therefore encourage opening market for new opportunities. The private data on customer, available to customer's/state's permitted institutions, should be reserved in smart contracts, verified with ZKP protocol among necessary counterparties, stored and timestamped as this permits necessary future alteration of information, retention for data protection and executing automatically essential payments not easily done on blockchain.

Every bank/PSP within its licence region should be linked to the ecosystem via application layer, which allows swift access to only relevant customer verified data, assess accompanied risks and mitigate them consequently. When the states know their citizens and corporations bank account numbers, the automatic notification to customer all banks and relevant smart contract control would provide always up-to-date data, eliminate current dated and post-act reporting and aid the tax handling. For instance, upon changes in tax residency, information that the customer is not filing or paying taxes and other data that could influence the necessary reporting, the authority can control that directly from special access smart contracts kept by the customer and/or the bank/PSP and may initiate tax transfer with applicable smart contract. Latter approach, shown on Figure 9 and Figure 10, would ease any type of tax collection, diminish double taxation issues and transferral of actually unnecessary data on persons who obey the law and concentrate on those who don't.

For customer, this way allows to fill in only one unified KYC in one state/region and keep it contents regularly updated as CDD, with verification from the agreed local authorities. Customers can use public KYC information also in their business activities, having better

control and automatization of paying for provided services, products or taxes via smart contracts and aid in this way preventing crime. They can use this data for their own audit trail, efficient their interactions and automate required reporting with tax authorities. Persons, which residence or birth country does not allow or afford digital identification, could, if ecosystems interoperability and state's risk tolerance allow, verify their identity through other secure and trustworthy global initiatives as ID2020, opening the reach to digital banking services of other regions.

Control layer

As to combating money laundering, the gatekeeper's role would be also in state's hand as depicted in Figure 7. Prior reaching the bank or service provider, all initiated customer payments would be filtered/screened via control layer handled by the consortium of authorities/FIUs, taken also into account customer's previous transaction behaviour. Control layer's content could be altered by states or regions due to upcoming laws, spotted trends, investigated crimes or similar required for crime prevention. Automatic result of the control layer analyses on customer's business data on public ledger and on accessible smart contracts, providing automated risk evaluation for the bank in deciding execution or rejection of the payment. The control layer screens the payment once – from order to execution, instead of current multiple screening and monitoring, and on existence of legal grounds, orders the bank to block or freeze the suspicious funds or automatically follow or trace back their movement with aid of other authorities/FIUs in global network.

This method allows the authorities and their supervisors executing control function, to partake direct overview of all payments related risks the state bears through its governed banks and their RBA stemming actions and investigate oddities and block/freeze funds on spot in both ways. States and regions joining the forces and know-how, just as encouraged by FATF, on implementing the common scenarios and hence be able to rely on trusted state's evaluation on particular customer or transaction, would efficient the current situation where every bank implements its own approach, control, screen and filter pre-act and monitor post-act and notify the FIU on its choice.

Most likely the false alerts created by current post-act monitoring tools of separate banks would be diminished in new pre-act joined screening-monitoring done with new technology possibilities, with broader knowledge and experience by the actual gatekeeper of the financial society and economy. This approach will effectuate also finding and closing current loopholes, spotting hot-spots and trends, predicting future development and to catch the funds and criminals on spot with evidence and money. This approach aids the states to define their RBA, consolidate and harmonise it with global governmental and banking sector without limiting banks to be with similar RBA within one region. With trustful party's verification, the cross-border banking would be as efficient and trusted as currently local.

This would encourage not only the cross-border interactions of regulators, but also businesses and banks resourcing the direct profit to all counterparties. The quality and quantity of current reports stem from the bank's monitoring regulations, past fears and possibilities – this would be also mitigated with proposed slant. Comparable approach can be used to any future new payment means as well. This process would also aid replacing other current mandatory reporting, such as termination of accounts with reasoning, loan/collateral/card/fraud/incidents reporting with automated notifications and would support enactments in other area challenges like consumer protection, risk transformation and structural reform.

Compliance and funding

The core risk management should be incorporated directly into the protocol, providing automatic compliance control. With the aid of new advanced technology and access to certain data, the gatekeeper's role in new ecosystem for customer's identification, transfer and assets handling with accompanied fraud control and possibilities to interact to pre-agreed extent with similar ones globally, presumably achieved in non-corrupt environment without any secret back-doors, allows states to be engaged in the 1st line of defence, rather than current "4th line" - being the last resource after the banks have exploited all their inside 3 lines of defences. To avoid misuse of accumulated of power, the controlling regulators in consortium or in cross-border rotational and selected way, as now auditors, would serve as the 2nd line.

The funds on implementing the over-regional monitoring system, taken into consideration the possibility to use current collected punishment fines to aid the development, would be covered with licence/regulators fees. When combining forces, its costs would prospectively be lesser than currently, where every bank bears those costs according to their RBA, hence the outcome of SARs is uneven in quality, prevents the actual criminals to be spotted and puts the whole country at risk. FIUs when joining forces with the aid of new technology, would also diminish their expenses and raise the result of catching funds and prosecuting criminals. One way to handle the question of current fines would be imposing them directly to the states and banks/PSPs who do not follow strong above anti-fraud DLT protocol or do not verify their citizens data correctly or miss stopping and freezing obvious criminal funds via control layer.

Future

DLT with its subcategories is quite raw to execute without further research from technological, security, and interoperability point of view. Control layer management technology separately and together with smart contract protocol, that regulates its validating and readability across borders, requires research and development. The more technical side knows of the problems and requirements accompanying financial institutions, the more tailor-made versions of DLT and other technologies interoperability possibilities will emerge. The regulators and authorities' knowledge on options efficient the state's risk resistance with DLT should rise after projects now in practice or in testing, reveal analysed outcome of results.

The additional questions open are from partakers willingness to analyse the probable change of current set-up, the possibilities and development of secure, scalable and confidentiality technology allowing efficiently prevented fraud, to utilisation of current systems and interoperability options with major partakers. If these all are successful, then finding the suitable and efficient consensus for selected protocols and standards (legal, technology) will be the next big challenge to face.

Most likely arising technologies like DLT will soon change all present banking system and therefore already now, the states joining forces in regions, should analyse the advantages the technology provides, study their options of cooperation with peers, technology experts and banks and take knowing-their-citizens, their businesses and companies with possibility for on-spot crime detection of transactions, more closely into their hands for safer and securer forthcoming financial opportunities.

7. Conclusions

Mapping of the banking institution's current processes in customer related mandatory reporting obligations stemming from the related dependencies for verification, screening and monitoring of transactions to spot suspicious and unusual activities, pictured an obvious pattern of difficulties, experienced by numerous credit institutions and their customers. To overcome these obstacles with the help of emerging technologies, several options were explored, how distributed ledger and its sub-category technologies could, in different types, be utilised.

Analyse of the distributed ledger technology's opportunities visible from existing projects and researches, lead to the most idealistic and probably efficient way to handle such interactions and prevent money laundering, terrorist financing and tax fraud within one or many regulative areas. Nevertheless, this is an option only when the technology and its soundness allow permissioned distributed ledger's gatekeeper's role, in verifying trustworthily the identity and other legally required data for customer and evaluative pre-transaction swift yet efficient screening control, to be shifted from banks to state authorities.

The proposed ecosystem would allow, if founded, contented and managed by cooperation of FIUs and/or respective authorities, under regulators control, within or cross-state, significant diminishment of any type of transaction related to tax evasion or money-laundering and participants time consummation and workload of necessary interaction for providing, analysing and reporting relevant data. Consequently, the same approach would presumably improve customer experience, its data quality, reduce its unnecessary multiplications and use, able execution of data protection related obligations and revert current active reporting by banks into pointed-to-know basis passive sharing. With unison management under regulators and FIUs cooperation protocols the aim of preventing money laundering and related illicit transactions within payment service providers of joined states is very likely to be achieved.

The further research opportunities of this approach are vast. From investigating, developing and testing standards and protocols of technology (including smart contracts), technical solution for managing the control layer, security and possibilities of interoperability with various types of existing and future ledgers, and payment services, studying political will and willingness of authorities to cooperate and fight crime with broader technological approach.

8. References

1. Wyman,O., Anthemis Group and Santander Innoventures (2015). The Fintech 2.0 Paper: rebooting financial services. Retrieved on 14.03.2018. http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

2. Basel Committee on Banking Supervision (2017). *Basel III: Finalising post-crisis reforms.* Retrieved 01.01.2018. https://www.bis.org/bcbs/publ/d424.pdf

3. Härle, P., Lüders, E., Pepanides, T., Pfetsch, S., Poppensieker, T. and Stegemann, U. (2010). *Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation*. McKinsey Working Papers on Risk, Number 26.

4. Federal Financial Analytics, Inc (2014). *The Regulatory Price-Tag: Cost Implications of Post-Crisis Regulatory Reform*. Retrieved 04.11.2017. http://www.fedfin.com/images/stories/client_reports/Cost%20Implications%20of%20Post-Crisis%20Regulatory%20Reform.pdf

5. Swan, M.(2015). "Blockchain". O'Reilly Media, Inc. First Edition.

6. Thomson Reuters (2016). *Know Your Customer Survey.* Retrieved 06.11.2017. https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

7. The Boston Consulting Group (2017). *Global risk 2017: Staying in course of banking.* Retrieved on 25.12.2017. http://image-src.bcg.com/BCG_COM/BCG-Staying-the-Course-in-Banking-Mar-2017_tcm9-146794.pdf

8. Oracle (2016). Know Your Customer: Product Overview. Oracle White Paper September 2016. Retrieved on 25.03.2018. http://www.oracle.com/us/industries/financial-services/fs-know-your-customer-wp-2655591.pdf

9. Demirguc-Kunt A., Klapper R., Singer D., Van Oudheusden P. (2014). The Global Findex Database 2014 Measuring Financial Inclusion around the World. World Bank Policy Research Working Paper 7255, World Bank, Washington, DC. Retrieved on 26.12.2017. http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf#page=3

10. World Federation of Exchanges database (2016). Table: *Listed companies total* Retrieved 26.11.2017. https://data.worldbank.org/indicator/CM.MKT.LDOM.NO

11. World Bank data catalogue (2016). *World Development indicators table 5.4 Stock Market*. Retrieved 26.12.2017. http://wdi.worldbank.org/table/5.4

12. Kushnir K., Mirmulstein L.M., Ramalho R. (2010). *Micro, Small, and Medium Enterprises Around the World: How Many Are There, and What Affects the Count?* World bank/IFC MSME Country Indicators 2010. Retrieved on 26.12.2017. http://www.ifc.org/wps/wcm/connect/9ae1dd80495860d6a482b519583b6d16/MSME-CI-AnalysisNote.pdf?MOD=AJPERES&CACHEID=9ae1dd80495860d6a482b519583b6d16

13. Keller, F. (2017). *New collaboration on trade finance platform built on blockchain*. IBM blog. Retrieved on 05.11.2017 https://www.ibm.com/blogs/blockchain/2017/10/new-collaboration-on-trade-finance-platform-built-on-blockchain/

14. Peyton,A.(2017). *IBM and eight banks unleash we.trade platform for blockchain-powered commerce*. BankingTech News. Retrieved on 06.01.2018. https://www.banking-tech.com/2017/10/ibm-and-eight-banks-unleash-we-trade-platform-for-blockchain-powered-commerce/

15. KYC-Chain website Retrieved on 27.12.2017 from https://kyc-chain.com/

16. Financial Conduct Authority Final Notice (2017). FCA website. Retrieved on 07.01.2018. https://www.fca.org.uk/publication/final-notices/deutsche-bank-2017.pdf

17. New York State Department of Financial Services (2017). *Consent on Deutche Bank mirror trading scheme.* Retrieved on 07.01.2018. http://www.dfs.ny.gov/about/ea/ea170130.pdf

18.European Central Bank (2017). *Stella report*. Retrieved on 06.01.2018 from https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf

19. The Monetary Authority of Singapore (2017). *Project UBIN Phase 2 – Re-imagining Interbank Real-Time Gross Settlement System using Distributed Ledger Technologies*. Retrieved on 26.12.2016. http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20Phase%202%20Reimagining%20RTGS.pdf

20. EuroFinance Corporate Treasury Network (2017). *The future of payments.* Retrieved on 01.01.2018. https://www.eurofinance.com/sites/default/files/PaymentReport2017_0.pdf

21. SWIFT website on their KYC register. Retrieved on 01.01.2018 from https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/our-kyc-solutions/the-kyc-registry/features

22. Lootsma, Y. (2017). *Blockchain as the Newest Regtech Application— the Opportunity to Reduce the Burden of KYC for Financial Institutions*. Banking & Financial Services Policy Report, August 1, 2017.

23. United Nations (2017). *Identity 2020*. Retrieved on 05.11.2017 from http://id2020.org/strategic-roadmap/ and http://id2020.org/digital-identity-1/

24. Gartner (2017). *Forecast: Enterprise IT Spending for the Banking and Securities Market, Worldwide, 2015-2021*. 3Q17 Update, October 30, 2017.Retrieved on 22.02.2018. https://www.gartner.com/document/3821565?ref=ddrec

25. Kaminski, P., Robu, K (2016). *A best-practice model for bank compliance.* Exhibit 1. Retrieved on 22.02.2018. https://www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-for-bank-compliance

26. Basel Committee on Banking Supervision (2005). *Compliance and the compliance function in banks*. Retrieved on 25.02.2018. https://www.bis.org/publ/bcbs113.pdf

27.Thomson Reuters (2017). *KYC challenges in 2017: A focus on the impact of globaal regulations in APAC*. Retrieved on 21.02.2018. https://risk.thomsonreuters.com/en/resources/special-report/kyc-challenges-2017-apac.html

28. U.S. Department of Treasury. FAQ section No 18. Retrieved on 24.02.2018. https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_lists.aspx

29. Financial Actions Task Force (2013). *Politically Exposed Persons (Recommendations 12 and 22)*. Retrieved on 27.02.2018. http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

30. World Bank, 2017. *Distributed Ledger Technology (DLT) and Blockchain*. FinTech Note No 1. Retrieved on 10.03.2018. http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

31. Deshpande A., Stewart K., Lepetit L., Gunashekar S. (2017). *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards*. BSI/RAND Europe. https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf

32. Brennan C., Lunn W (2016). *Blockchain. The Trust Disruptor*. Credit-Suisse Research Equity. Retrieved on 11.03.2018. http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf

33. Financial Actions Task Force (2014). *Guidance for a Risk-Based Approach - The Banking Sector.* Retrieved on 24.03.2018. http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

34. OECD (2017). *Common Reporting Standard User Guide, in Standard Automatic Exchange of Financial Account Information in Tax Matters*, Second Edition, OECD Publishing, Paris. Retrieved on 31.03.2018. http://dx.doi.org/10.1787/9789264267992-10-en

35. Department of the Treasury Internal Revenue Service (2017). *FATCA XML Schema v2.0 User Guid*e. Publication 5124 (4-2017) Catalog Number 65544H. Retrieved on 31.03.2018 https://www.irs.gov/pub/irs-pdf/p5124.pdf

36. Moyano J.P., Ross, O. *KYC Optimization Using Distributed Ledger Technology*. Bus Inf Syst Eng 59(6):411–423 (2017). Retrieved on 13.01.2018. https://doi.org/10.1007/s12599-017-0504-2

37. Pisa M., Juden M. (2017). *Blockchain and Economic Development: Hype vs Reality*.CDG Policy Paper 107. Retrieved on 12.04.2018. https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf

38. Cermeño J.S.(2016). *Blockchain in financial services: Regulatory landscape and future challenges for its commercial application*. BBVA Research Working paper, 16/20. Retrieved on 13.04.2018. https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf

39. A report by the UK Government Chief Scientific Adviser (2016). *Distributed Ledger Technology: beyond block chain.* OGL GS/16/1. Retrieved on 15.04.2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

40. Kosba A., Miller, A.(2016). *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*. 2016 IEEE Symposium on Security and Privacy. Retrieved on 15.04.2018. https://ieeexplore-ieee-org.ezproxy.utlib.ut.ee/abstract/document/7546538/?part=1

41. Lewis A. (2017). *A Gentle Introduction to Self-Sovereign Identity*. Blog Bits on Blocks. Retrieved on15.04.2018. https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

42. Finextra Blog *KYC and Blockchain*. 30.03.2017. Retrieved on 12.04.2018. https://www.finextra.com/blogposting/13903/kyc-and-blockchain

43. Juskalian, R. (2018). *Inside the Jordan refugee camp that runs on blockchain*. MIT Technology Review 12.04.2018. Retrieved on 15.02.2018. https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

44. GLEIF and McKinsey Company (2017). *The Legal Entity Identifier: The Value of the Unique Counterparty ID- White Paper.* Retrieved on 19.04.2018. https://www.gleif.org/en/about-lei/mckinsey-company-and-gleif-creating-business-value-with-the-lei

45. G20. https://www.g20.org/en/g20/what-is-the-g20

46. Financial Stability Board. http://www.fsb.org/

47. World Economic Forum, (2018). *The Known Traveller Unlocking the potential of digital identity for secure and seamless travel.* Retrieved on 19.04.2018. http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf

48. Decentralized Identity Foundation. http://identity.foundation/

49. Patel, N. (2017). *Blockchain KYC/AML Utilities for International Payments: A Regulatory Solution for Anti-Money Laundering and Financial Inclusion?* Retrieved on 21.04.2018. https://www.r3.com/wp-content/uploads/2018/04/blockchain_kyc_aml_utilities_R3-1.pdf

50. Dentsu, iSiD (2017). *CORDA introduction to case studies*. Retrieved on 18.04.2018. https://www.jipdec.or.jp/sp/topics/event/u71kba000000an5u-att/10_isid.pdf

51. Stark, J. (2017*). Applications of Distributed Ledger Technology to Regulatory and Compliance Processes. R3 White Paper.* Retrieved on 04.04.2018. https://www.r3.com/wp-content/uploads/2017/07/apps-reg-compliance_R3.pdf

52. Yang, D., Gavigan, J, Wilcox-O'Hearn, Z. (2016). *Survey of Confidentiality and Privacy Preserving Technologies for Blockchains.* R3 Research. Retrieved on 21.04.2018. https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/58c0282fcd0f68b2ab013596/1488988208799/R3_Confidentiality_and_Privacy_Report.pdf

53. Rivest, R.L, Shamir, A., Tauman, Y. (2001). *How to Leak a Secret*. Advances in Cryptology — ASIACRYPT 2001. Retrieved on 21.04.2018. https://link.springer.com/chapter/10.1007%2F3-540-45682-1_32

54. Staples, M, Chen, S., Falamaki, S. *et al*. (2017). *Risks and opportunities for systems using blockchain and smart contracts.* Data61 (CSIRO). Sydney. retrieved on 12.04.2018. https://www.researchgate.net/publication/320619389_Risks_and_opportunities_for_systems_using_blockchain_and_smart_contracts

55. Kwori blog, 30.05.2016. *Deleting information from Distributed Ledger or Blockchain*. Retrieved on 19.02.2018. http://www.kwori.co.uk/blog/2016/5/30/deleting-information-from-a-distributed-ledger-or-blockchain

56. Vranken, A. (2017). *Actually there could be a way to delete data on a blockchain*. Medium corporation web. Retrieved on 19.02.2018. https://medium.com/@artusvranken/actually-there-could-be-a-way-to-delete-data-on-a-blockchain-df62964bd927

57. Bacon, J.,Bacon, M., Johan, D. (2017). *Blockchain Demystified*. Queen Mary School of Law Legal Studies Research Paper No. 268/2017. Retrieved on 21.04.2018. SSRN: https://ssrn.com/abstract=3091218

58. Peters, G.W., Vishnia, G.R. (2016). *Blockchain Architectures for Electronic Exchange Reporting Requirements: EMIR, Dodd Frank, MiFID I/II, MiFIR, REMIT, Reg NMS and T2S*. Retrieved on 22.04.2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832604

59. Warnez , J.(2017).*Revenue registration and automatic taxation for platform businesses on blockchain.* Copenhagen Business School. Retrieved on 22.04.2018. https://www.researchgate.net/profile/Jens_Warnez/publication/321379898_Revenue_registration_and_automatic_taxation_for_platform_businesses_on_blockchain/links/5a1fcb80aca272cbfbc32548/Revenue-registration-and-automatic-taxation-for-platform-businesses-on-blockchain.pdf
60. Schwartz, D., Youngs, N., Britto, A. (2014). *The Ripple Protocol Consensus Algorithm.* Ripple Labs Inc, 2014 Retrieved on 22.04.2018. https://ripple.com/files/ripple_consensus_whitepaper.pdf
61. Mazieres, D. (2016). *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus.* Stellar Development Foundation. Retrieved on 22.04.2018. https://www.stellar.org/papers/stellar-consensus-protocol.pdf
62. Hileman, G., Rauchs, M. (2017). *Global Blockchain Benchmarking Study (September 22, 2017).* Retrieved on 25.04.2018. https://ssrn.com/abstract=3040224
63. https://litecoin.org/
64. https://www.bitcoin.com/
65. https://www.ethereum.org/
66. https://www.hyperledger.org/
67. https://www.ibm.com/blockchain/hyperledger.html
68. https://ripple.com/
69. https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html
70. https://docs.corda.net/
71. European Commission Press Release on the adoption by the European parliament of the 5th Anti-Money laundering Directive.19.04.2018. Retrieved on 24.04.2018. http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm
72. FATF (2012-2018). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. FATF, Paris, France. Retrieved on 28.04.2018. www.fatf-gafi.org/recommendations.html
73. FATF (updated 30.04.2018). *Consolidated assessment rating*. Retrieved on 01.05.2018. http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf
74. Meyer, D. (2018). *The privacy Advisor – Blockchain technology is on a collision course with EU Privacy Law.* IAPP News 27.02.2018. Retrieved on 23.04.2018. https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/
75. Baird, L. (2016). *The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance.* Swirlds Tech Report Swirlds-Tr-2016-01. Retrieved on 02.05.2018. http://www.leemon.com/papers/2016b.pdf
76. OECD (1995). *Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved on 05.05.2018. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
77. Phunia, P. (2017). *Consortium of banks, together with IMDA Singapore, completes proof-of-concept for ASEAN's first industry KYC Blockchain.* Retrieved on 27.03.2018. https://www.opengovasia.com/articles/8093-consortium-of-banks-together-with-imda-completes-proof-of-concept-for-aseans-first-industry-kyc-blockchain
78. OECD (2018), *Standard for Automatic Exchange of Financial Information in Tax Matters - Implementation Handbook - Second Edition*, OECD, Paris. Retrieved on 02.02.2018. http://www.oecd.org/tax/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-offinancial-account-information-in-tax-matters.htm

79. FATF (2013-2018), *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*, updated February 2018, FATF, Paris, France. Retrieved on 02.04.2018. www.fatfgafi.org/publications/fatfrecommendations/documents/fatfissuesnewmechanismtostrengthenmoneylaunderingandterroristfinan cingcompliance.html
80. http://www.bankchaintech.com/
81. Oh,J, Shong, I.(2017). *A case study on business model innovations using Blockchain: focusing on financial institutions*, Asia Pacific Journal of Innovation and Entrepreneurship, Vol. 11 Issue: 3, pp.335-344. Retrieved on 25.03.2018. https://doi-org.ezproxy.utlib.ut.ee/10.1108/APJIE-12-2017-038
82. FinCEN News. *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger.* Retrieved on 22.04.2018. https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual
83. Chatterjee, S. *HSBC says performs first trade finance deal using single blockchain system.* Reuters Business News 14.05.2018. Retrieved on 14.05.2018. https://www.reuters.com/article/us-hsbc-blockchain/hsbc-says-performs-first-trade-finance-transaction-using-blockchain-idUSKCN1IF01X
84. Woodsome, J., Ramachandran, V.(2018). *Fixing AML Can New Technology Help Address the De-risking Dilemma?* Center for Global Development. Retrieved on 17.05.2018. https://www.cgdev.org/sites/default/files/fixing-aml-can-new-technology-help-address-de-risking-dilemma.pdf
85. Standards Australia ISO/TC 307 *Blockchain and distributed ledger technologie*s Retrieved on 18.05.2018. https://www.iso.org/committee/6266604.html
86. Anjum,A, Sporny, M., Sill, A. (2017). *Blockchain Standards for Compliance and Trust.* Retrieved on 04.04.2018.IEEE Cloud Computing (Volume: 4, Issue: 4, July/August 2017) https://ieeexplore-ieee-org.ezproxy.utlib.ut.ee/document/8066010/
87. Schueffel, P. (2017) *Alternative Distributed Ledger Technologies: Blockchain vs. Tangle vs. Hashgraph - A high-level overview and comparison.* Retrieved on 02.05.2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144241
88. Cachin, C. *et al* (2017) *Blockchains and consensus protocols*. IBM Research 2017. Retrieved on 18.05.2018. https://cachin.com/cc/talks/20170908-blockchain-edcc.pdf
89. Cachin, C., Vucolić, M. (2017). *Blockchain Consensus Protocols in the Wild, v2.* Retrieved on 18.05.2018. arXiv:1707.01873v2
90. Hughes, D. (2018). *Why DAGs Don't Scale Without Centralization*. Radix DLT 9.03.2018. Retrieved on 17.05.2018. https://www.radixdlt.com/post/dags-dont-scale-without-centralization
91.Nguyen, W. (2018). *Hedera Hashgraph Review – the Blockchain Killer?* Bitcoin For Beginners 10.04.2018. Retrieved on 17.05.2018.https://www.bitcoinforbeginners.io/hedera-hashgraph-review/
92. Meguerditchian, V. (2017). *Roadmap for Blockchain Standards Report- March 2017. Standards Australia*. https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx
93. International Telecommunication Union. Focus Group on DLT. https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx
94. R3 CEV Ltd letter to Financial Industry Regulatory Authority. Re: Distributed Ledger Technology: Implications of Blockchain for the Securities Industry. Retrieved on 19.05.2018. https://www.finra.org/sites/default/files/Blockchain-R3-Comment.pdf
95. Hearn, M. (2016). *Corda: A distributed ledger.* Corda Whitepaper Version 0.5. Retrieved on 24.04.2018. https://docs.corda.net/_static/corda-technical-whitepaper.pdf

96. Buterin, V. (2016). *Chain Interoperability*. R3 Reports 09.09.2016. Retrieved on 19.05.2018.https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf
97. Tangle IOTA. *Identity project*. Retrieved on 17.05.2018. https://forum.iota.org/t/identity-of-people/2629
98.Shueffel, P. (2018). 10 years Blockchain. *The Race is on: Blockchain vs. Tangle vs. Hashgraph.* FinTechNews 19.02.2018. Retrieved on 17.05.2018. http://fintechnews.sg/16989/blockchain/10-years-blockchain-the-race-is-on-blockchain-vs-tangle-vs-hashgraph/
99. Ahlm, H. (2018). *Traditional block chain technology is being disrupted.* Linkedin Pulse 09.02.2018. Retrieved on 17.08.2018. https://www.linkedin.com/pulse/traditional-block-chain-technology-being-disputed-distributed-ahlm
100. Baird, L., Harmon, M., Madsen, D. (2018). *Hedera: A Governing Council & Public Hashgraph Network.* Hedera Whitepaper v.1.1. Updated 18.05.2018. Retrieved on 19.05.2018. https://s3.amazonaws.com/hedera-hashgraph/hh-whitepaper-v1.1-180518.pdf
101. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) *Where Is Current Research on Blockchain Technology?* A Systematic Review. PLoS ONE 11(10): e0163477. Retrieved on 19.05.2018. https://doi.org/10.1371/journal.pone.0163477
102. Mills, D., Wang, K., Malone, B., Ravi, A., Marquardt, J., Chen, C., Badev, A., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellithorpe, M., Ng, W. and Baird, M. (2016). *Distributed ledger technology in payments, clearing, and settlement.* Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System. Retrieved on 20.05.2018. https://doi.org/10.17016/FEDS.2016.095.

I. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Kristin Sõgel**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Distributed Ledger Technology and External Mandatory Reporting in Banking Industry,

supervised by Fredrik Payman Milani,

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **21.05.2018**