Civil Liability for Damaging of Goods Following the Application of the “Smart Contracts” in the Context of International Sale and Carriage of Goods Industry: The UK and German perspective

Khotulev Kirill (SNR 2013211**)**

Supervisors:

Dr B. Zhao, LLM

M.A. Paun, LLM

Tilburg, August 2018

Table of Contents

List of Abbreviations

DAO - Decentralized autonomous organization

IoT – Internet of things

ISCG – International sale and carriage of goods

PoW – Proof of work

SC – Smart contract

SCC – Smart contract code

Introduction

1.1. Background and problem statement

As Ralph Waldo Emerson, a famous US philosopher, once pointed out: "Our distrust is very expensive".[1] Even though his words were addressing a broad range of issues in human relationships, without any doubt, contractual relations could be named among the fields affected by the distrust.[2] Indeed, the distrust and transaction costs in contractual relations appear from the fact that contracting parties do not have control over each other and thus could not be sure of their capabilities, experience and real intentions of each other.[3] This "veil of ignorance" affects both pre-contractual and post-contractual stages of the contract life cycle. In the pre-contractual relations, the distrust hinders the negotiations and raises their costs, because the parties have to fund the participation of legal advisors and other consultants in the process of the negotiation, in order to mitigate potential risks connected with the normal contract performance.[4] In the performance stage of the contract, even closest partners may not be sure that their contractual relations will not end in a default of payment or provision of goods/services by one of them.[5]

The distrust gap widens even further in the sphere of international contracts. As parties of such contracts are established and/or have their main business interests in different countries, they are unaware of each other. If compared to the situation with the contract parties originating from one country, the international contract counterparts have even less information about each other, because they could be prevented from gaining access to this data either by national legislation or by not knowing the reputation of each other. Furthermore, such counterparts speak different languages, which makes the contract drafting complicated, for the meaning of the same notions and phrases may differ depending on the language.[6] Finally, the rules governing international contracts originate from different national legal systems, which could be contradictory to each other and could be unknown to the parties.[7] Therefore, abovementioned proves that the "veil of ignorance" between the parties of international contracts is bigger and thus the distrust between such counterparts is harder to overcome, which entails extra transactional costs for the parties.

The importance of solving the distrust problem in the sphere of international contracts becomes even more apparent if taking into account the economic statistics. As shown by the analysis of the World Bank, the average of 60% share of the world GDP is occupied by international trade, while about half of this share is represented by the export

[1] Ralph W Emerson, 'A Lecture read before the Mechanics' Apprentices' Library Association, Boston' (Ralph Waldo Emerson, 25 January 1841) <https://emersoncentral.com/texts/nature-addresses-lectures/lectures/man-the-reformer/> accessed 3 August 2018

[2] Zoltan Bakucs and Imre Ferto, *The role of trust in contractual relationships* (Warwick University, Coventry, UK 2013) 2

[3] Simon Deakin and others, ''Trust' or Law? Towards an Integrated Theory of Contractual Relations between Firms' [1994] 21(3) Journal of Law and Society 336

[4] Oliver E Williamson, *The Economic Institutions of Capitalism* (Collier Macmillan Publishers 1985) 20; Bakucs and Ferto (n 2) 4

[5] Williamson (n 4) 20

[6] Marcia E Greenberg, 'International Contracts: Problems of Drafting and Interpreting, and the Need for Uniform Judicial Approaches' [1987] 5(2) Boston University International Law Journal 363-364

[7] Adrian Briggs, *The Conflict of Laws* (3 edn, Oxford University Press 2013) 5, 8-9, 11, 19

of goods and services.[8] Consequently, as both international trade and export of goods and services are dependent on international contracts, for it is the only mean for counterparts from different countries to set their relations legally, the mitigation of the distrust issue, intrinsic to the international contracts, may lead to the considerable world economy boost.

Among the possible answers to the distrust issue in the domain of international contracts, some authors and companies propose the implementation of smart contracts [SC] and internet of things [IoT] devices.[9] In essence, this idea is that SCs and IoT devices could be invoked to fully or partly replace international contracts and remove the distrust in the contractual relations by the incorruptible precision of the computer code and high trust mechanisms behind the SCs technology.[10] This solution to the distrust issue is explained below.

In general, SC is a computer program, which operates automatically after being started by its developers/users.[11] While there are different functions which could be performed by such virtual machines, with regard to contractual relations this kind of programs could include "if…then" commands, upon which regular contractual clauses could be transferred into computer code and performed by the machine itself.[12] Subsequent to the coding of the SC, it is connected to the IoT equipment representing different sensors and mechanisms in real world. This allows the SC to receive information from the IoT devices and send commands to them.[13] Wherein, the blockchain technology, underlying the SCs, provides protection of the SCs code and their commands from their modification by anyone including contract.[14] This means that the performance of the contract encoded in the SC goes in real life precisely as stated in the SC without any alterations possible.

[8] Worldbank, 'Trade (% of GDP)' (*Worldbank.org*, 1 January 2018) <https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS> accessed 5 August 2018; Worldbank, 'Exports of goods and services (% of GDP)' (*Worldbank.org*, 1 January 2018) <https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS> accessed 5 August 2018

[9] Helen Eenmaa-Dimitrieva and Maria J Schmidt-Kessen, 'Regulation through code as a safeguard for implementing smart contracts in no-trust environments' [2017] 2017(13) European University Institute Working Paper Law 16; Kevin Werbach, 'Trust, But Verify: Why the Blockchain Needs the Law' [2018] 33(2) Berkley Technology Law Journal 538; Sammy Naji, 'Smart Contracts: What Are They and What Do They Mean for International Trade?' (International Law & Practice, 18 December) <http://ncbarblog.com/smart-contracts-what-are-they-and-what-do-they-mean-for-international-trade/> accessed 5 August 2018; Chris Skinner, 'Five Standout Start-Ups Focused Upon Blockchain Trade Finance' (Chris Skinner's Blog, 2017) <http://thefinanser.com/2016/08/fivestandout-start-ups-focused-upon-blockchain-trade-finance.html/> accessed 5 August 2018; IBM, 'Implement your first IoT and blockchain project' (*Watson Internet of Things*, 21 June 2017) <https://www.ibm.com/internet-of-things/platform/private-blockchain/> accessed 5 August 2018; Skuchain.com, 'Brackets' (*Skuchain.com*, 15 November 2017) <http://www.skuchain.com/brackets/> accessed 5 August 2018

[10] Ibid

[11] Kristian Lauslahti and others, 'Smart Contracts – How will Blockchain Technology Affect Contractual Practices?'[2017] 1(68) Research Institute of the Finnish Economy Reports 3-4

[12] David M Adlerstein, 'Are Smart Contracts Smart? A Critical Look at Basic Blockchain Questions' (Coindesk, 26 June 2017) <https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract/> accessed 5 August 2018

[13] Vikram Dhillon and others, *Blockchain Enabled Applications* (Apress Berkely 2017) 33-35

[14] Max Raskin, 'The Law and Legality of Smart Contracts' [2016] 2017(304) Georgetown Law Technology Review 326-327

Consequently, one may find a number of benefits, which implementation of SCs and IoT into the international contracts entails with regard to the distrust problem. First, the aforementioned problem of differences in languages between the parties to the international contracts is mitigated by the fact that SCs are computer programs written in a universal computer language that is not dependent on a specific country.[15] Second, in principle, the distrust concern on the performance stage of the contract is mitigated, for the contract parties could expect the precise performance of the contract through the SC. For example, delivery of goods/services from one party and payment from another will take place in accordance with the code of the SC.[16] Third, the pre-contractual need for information about material situation of a counterpart and his intentions becomes obsolete, because the SC may be performed only as stated in its code preventing any negative influence from the wrong choice of a counterpart.[17] At last but not the least, the SC and IoT implementation further mitigates the costs of the contracting by removing the involvement of intermediaries such as banks and courts, for their enforcement functions are performed by the SCs and IoT.[18] Therefore, all these benefits combined could potentially decrease the overall costs of negotiating and performing of contracts. This will allow the traders to gain more profits and thus will boost the international economy.

Nevertheless, at this point of technological advancement, SCs and IoT could be implemented only to a limited number of international contracts, among which international sale and carriage of goods [ISCG] may be named. The latter is proved by the case, where the first ISCG contract implementing a SC on the sale of 100000 USD worth butter and cheese was concluded between a Seychelles enterprise and Ornua - Israeli cheese manufacturer.[19] This SC was performed in conjunction with the IoT system comprised of goods tracking equipment, which marked the arrival of the goods to the destination point triggering automatic payment to the seller.[20] More elaborate solutions on the ISCG with the SC application could be provided by the IBM Watson IoT or Skuchain platforms virtualizing data from different real-time IoT sensors into the language of SCs, in its turn, facilitating performance of the ISCG contracts.[21]

[15] Even though instructions according to which the contract is drafted could be in different languages, the final code of the SC will be in a computer language that does not allow its twofold interpretation. This allows parties to check whether the final code of the SC answers their interests and to be sure that its execution will go only as written in the SC’s code. Malcolm Campbell-Verduyn, Introduction in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018) 10

[16] Logistics bureau, 'How Blockchain Can Transform the Supply Chain' (*Logistics Bureau*, 15 November 2017) <https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/> accessed 5 August 2018; Gazelle information technologies, 'Supply Chain Shipment Tracking Using Ethereum Blockchain Based Smart Contracts' (*Gazelle Information Technologies*, 14 September 2017) <https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/> accessed 5 August 2018

[17] Alexander Savelyev, ‘Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law’ [2016] 2016(71) Higher School of Economics Research Papers 5-6

[18] Kevin Werbach and Nicolas Cornell, ‘Contracts Ex Machina’ [2017] 2017(67) Duke Law Journal, 338-339

[19] Pravo.ru, 'Юридическая матрица: когда наступит время блокчейна' (*Pravoru*, 21 June 2017) <https://pravo.ru/review/view/141356/> accessed 5 August 2018

[20] Ibid

[21] IBM, 'Implement your first IoT and blockchain project' (n 9); Skuchain.com, ' Brackets ' (n 9)

It would be still overreaching to arrive at the conclusion from the aforementioned that SCs and IoT could totally replace conventional contracts in the ISCG industry,[22] but the application of these systems in the form of an escrow in parallel to the conventional contracts could be an option.[23] By some authors, an escrow in the form of a SC is represented by a SC-based system relatively close to the concept existing in the modern banking,[24] i.e. the construction which through the bank intermediary establishes high trust payment for the services or goods delivered.[25] In essence, the conventional escrow works as following: one of the parties to the contract opens an escrow account in the bank and transfers money to it, which could be withdrawn only by the other contracting party against the completion of the performance of the contract checked by the bank.[26] Conversely, the SC-based escrow does not need an intermediary and both the transfer of payment for the delivery and checking of the performance are conducted by the SC.[27] Therefore, previously described benefits of the SCs regarding combating distrust could be implemented as a technical instrument in parallel to the ISCG contract through the automation provided by the SC and IoT acting in the form of an escrow.

Nevertheless, even though the proposal to implement SC and IoT system to the ISCG contracts seems to be possible and beneficial for the ISCG contracts and world economy, the authors of this proposal and other literature might overlook following complications triggered by the suitability of SC and IoT to contract law of different countries.[28] First, the issues may arise from the nature of SCs, since they are computer programs and are subject to the same flaws as bugs in the code and hacking attacks.[29] Consider the situation where the SC is implemented in the form of an escrow to the ISCG contract and gives commands influenced by bugs/hacking to the IoT devices. This situation may lead to either damaging or destruction of goods and subsequent losses for the buyer. It is not obvious in this case that the buyer will be able to claim damages for the mentioned losses. This is so, because the seller may succeed in showing that he was not in control of the aforementioned flows of the SC and thus will avoid liability by invoking existing exemptions from liability, and *force majeure* clauses.[30]

Second, the situation grows to another level with the third parties involvement. Among such one could name developers of the SC, actions of which in most occasions do not equal to the sellers’ actions. Not only the complex application of liability rules described above would become more intricate, but also the question could arise whether the buyer is entitled to claim damages, from whom and in which circumstances. These

[22] Raskin (n 14) 322-329

[23] Werbach and Cornell (n 18) 337-343

[24] Ibid 24-26

[25] Patrick E O'Neil, 'The Escrow transactional method' [1986] 11(4) Computer Corporation of America Transactions on Database Systems 410-411

[26] Kate Davies and Helena Nathanson, 'Standard term escrow agreements: the potential pitfalls for depositors and agents alike' [2013] 28(10) Butterworths Journal of International Banking and Financial Law 587-588

[27] Werbach and Cornell (n 18) 336-338

[28] Eenmaa-Dimitrieva and Schmidt-Kessen (n 9) 16; Skuchain.com, 'Brackets' (n 9); Naji (n 9)

[29] Cem Kaner and others, *Testing Computer Software* (2edn, Wiley 1999) 7; Howard Shrobe, 'It is possible to design a computer system that can't be hacked' (CNBC, 30 September) <https://www.cnbc.com/2016/09/30/it-is-possible-to-design-a-computer-system-that-cant-be-hacked-commentary.html> accessed 5 August 2018

[30] Anthony G Guest, Exemption Clauses in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017) 1212

concerns are raised as the rules of contract and tort actions are applicable on the different stages of ISCG contract, while the rules regarding third parties liability may also preclude the buyer from action choice.[31]

Finally, the additional layer of complexity dwells upon the different jurisdictions chosen as applicable law for the ISCG contracts. The ISCG contracts in most of the situations are subject to different jurisdictions chosen by the parties as applicable law.[32] This means that regulation of the same issues connected with SC and IoT application may differ depending on the chosen applicable law.

Thus, this gap in the literature should be closed before application of SC and IoT even in their limited escrow format becomes over-present in the ISCG. Otherwise, there will be a possibility that the SC-IoT system, dedicated to battle the distrust between international contract parties, would instead create distrust and thus add transaction costs for the contract parties. In order to prevent the SC counter-distrust mechanism from becoming equally or more expensive for the contract parties than the normal distrust situation in ISCG contracts, it is necessary to assess whether the nature of SCs would be suitable to both the contemporary contractual and tort legislation, and the need of high trust environment.

While considering this, emphasis is to be placed on finding a jurisdiction, if any, mostly suitable for the implementation of the SC and IoT. This search is made among the most widely applicable jurisdictions in the ISCG contracts, since these jurisdictions already provide most beneficial conditions for the regulation of ISCG aspects not connected with SCs application. Therefore, if any of these jurisdictions could accommodate application of the SCs, it will be possible to state that these jurisdictions are sufficient to become applicable law in an ISCG contract implementing SCs. The laws analyzed are of the United Kingdom [UK] and Federal Republic of Germany [FRG/Germany], for they are the most commonly used ones as applicable law in the ISCG contracts.[33] In its turn, analysis of these jurisdictions regarding tort law issues is explained by the practical necessity for the parties of the ISCG contract to subject these issues to the same jurisdictions as contract issues in order to avoid depecage.[34] Subjecting tort law issues to a certain jurisdiction at the discretion of the contract parties is allowed by the legislation of the European Union.[35]

[31] Ruben de Graaf, 'Concurrent Claims in Contract and Tort: A Comparative Perspective' [2017] 2017(4) European Review of Private Law 716-722

[32] Gilles Cuniberti, 'The International Market for Contracts: The Most Attractive Contract Laws' [2014] 34(3) Northwestern Journal of International Law & Business 459

[33] Ibid

[34] International private law understands depecage as a situation in which one legal issue is subjected to two or more jurisdictions. Such a situation is considered to be negative and both legislations and private parties try to avoid depecage. Therefore, the parties to the ISCG contract would like to avoid depecage by choosing one jurisdiction regulating both tort and contract claims especially in the situation where a SC damages goods both under the tort and contract law. See more: Craig M Gertz, 'The Selection of Choice of Law Provisions in International Commercial Arbitration: A Case for Contractual Depecage' [1991] 12(3) Northwestern Journal of International Law & Business 178-180; Willis LM Reese, 'Dépeçage: A Common Phenomenon in Choice of Law' [1973] 73(1) Columbia Law Review 63-75

[35] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the Law Applicable to Non-Contractual Obligations (Rome II) [2007] OJ 2 199/40 s 14(1)(b)

UK and FRG jurisdictions are assessed on the basis of the balance of interests of sellers and buyers which should be maintained in case of the damage of goods by the alleged automated system. On the one hand, interests of the buyer are considered in the possibility to gain remuneration for the described damage. On the other hand, the ideology of high trust between the parties to the contract using SC should not be put aside as this ideology is the key interest of the business society seeking to decrease transactional costs in international trade and also a reason for its utilization by the seller.[36]

1.2. Thesis question and sub-questions

Thus, considering that there is such a gap in the literature and potential demand from the business community, the research question is as following: **Whether UK or German law, if at all suitable, better suits the situations where an unintended execution of a SC as a performance instrument in an ISCG contract leads to the damaging of goods?**

In order to facilitate answering the main question three sub-questions were developed:

1. *How could smart contracts be used as an instrument of performance in the international sale and carriage of goods contract and what could be the reason for the unintended execution of the SCs leading to the damaging of goods in such use cases?*

2. *Who could be held liable for the damage of goods in that event and what liability could be imposed on that responsible person?*

3. *Whether the UK or FRG jurisdiction, if at all suitable, is to be considered better suitable as applicable law in ISCG contract utilizing SCs as an instrument of performance in the sense of necessity to establish balance between the interests of sellers, buyers and the business society as a whole?*

1.3. Methodology

As the aim of this thesis is to figure out whether contemporary legislation in the area of ISCG is compatible with liability calls provided by SCs, if implementation of SCs would be found efficient, analysis of the contemporary law regarding blockchain technology and ISCG is crucial for the research. Legal examination of the SCs unintended execution leading to the damaging of goods is necessary to find out whether any of the actors could be claimed liable and to establish the type and extent of their liability. It further facilitates finding whether the interests of the abovementioned stakeholders are balanced as it shows who of them sustains losses and who gains benefit as a result of a damage claim. Since there is no literature directly assessing these issues regarding the application of SCs in the context of the ISCG contracts, the analysis is based on two following types of literature. First, literature explaining technological side of the SCs application is analyzed in order to figure out the liability issues posed by the automated nature of the SCs and their software essence. Second, legal literature explaining general concepts of liability in the ISCG context is analyzed in order to figure out how these

[36] Bakucs and Ferto (n 2) 4

concepts apply to the liability issues raised by the implementation of the SCs to the ISCG contracts.

In achieving the thesis goal, these legal and technological materials are scrutinized following the doctrinal research, for it provides necessary tools for analysis of practical situations. In this case, this is damaging of goods as a result of unintended execution of the SC. To facilitate the analysis of the research question two case studies are provided in chapters 3 and 4. Both of the case studies represent use cases of SCs as instruments for the performance of the ISCG contract as provided by IBM Watson IoT or Skuchain platforms. Potential complications arising from the SCs damaging goods in an ISCG contract are shown through these case studies. Furthermore, as no existing literature specializes on the liability issues stemming from the application of the SCs, the main approach of this research is to examine whether application of the SCs is adequately addressed by broader concepts of contract and tort liability in the ISCG domain. It should be also noted that while no court cases concerning either SCs or Blockchain with regard to the thesis topic exist, case analysis is limited to cases explaining the abovementioned concepts in relation to the SCs technology.

Apart from doctrinal research, comparative method is also used in order to achieve an educational goal,[37] i.e. to provide lawyers with the knowledge of which jurisdictions, if any, could suit SCs application in the ISCG contracts. The comparative method in this research also achieves the lawmaking goal by allowing the lawmakers to see the benefits and drawbacks of the analyzed jurisdictions and to implement this knowledge to the regulation of the SCs in the future.[38] These goals are achieved through the application of the functionality principle of the comparative method entailing the analysis of how successful different jurisdictions are in regulating certain legal problems and what means they use for this.[39] Therefore, different legal institutes of each compared jurisdiction are checked for their ability to effectively regulate SCs in ISCG contracts and to establish the balance of interests between the parties of such contracts.

As provided above, the laws analyzed are of the UK and FRG. Apart from the fact that these jurisdictions are the most commonly used as applicable law in ISCG contracts,[40] the UK and FRG are representatives of two largest legal systems, i.e. common law and continental legal system. Therefore, comparison of their legal provisions may provide an overall understanding of possible approaches to the SCs liability issues in the majority of other states. Moreover, the chosen legal systems are known for having different levels of freedom of contract construction with common law having less restrictions than continental law.[41] The latter fact would help to scrutinize the practical possibility of subjecting SCs to legal systems with larger contractual freedoms and their enforceability in jurisdictions with less contractual freedoms. In relevant parts, international contract law is studied and used solely as a corroborative source for proving research statements.

Finally, it should be noted that no analysis of product liability is conducted, for the research context is centered around international trade and thus addresses questions

[37] Konrad Zweigert and Hein Kötz, *An Introduction to Comparative Law* (3 edn, Calderon Press 1998) 29-30

[38] Ibid 36-37

[39] Ibid 68-69

[40] Cuniberti (n 32) 459

[41] Ibid 504-505

mostly faced by legal entities, but not the individuals, who are exclusively protected under product liability laws in both jurisdictions.[42] The research also does not go into detail with issues connected with restitution as they are not supposed to be affected by the specific nature of the SCs.[43]

1.4. Chapters outline

If taking into account everything abovementioned, the following chapter provides the basis for further analysis of the matters in question by describing the essence of the SCs technology, its possible applications in the ISCG industry and also the flaws of the SCs relevant to the liability issues in the ISCG contracts. Subsequently, Chapter 3 dwells upon the analysis of liability for application of the SC-IoT system in the ISCG contract with the UK jurisdiction as applicable law. Main emphasis is made on the SCs' flaws discovered in Chapter 2 and precluding the buyer from claiming liability for the destruction or damage of goods by the SC-IoT system. Finally, Chapter 4 compares results of the UK jurisdiction analysis with the regulation of liability in the FRG jurisdiction under the comparable conditions. This allows to figure out the better of the two, if any, applicable law for the ISCG contract implementing a SC-IoT system.

[42] Consumer Protection Act 1987 s 5(3); Nicholas J McBride and Roderick Bagshaw, *Tort Law* (5 edn, Pearson Education Limited 2015) 395, 401-402; Ralf Grote, Product Liability Under German and European Law. in Wendler and others (eds), *Key Aspects of German Business Law* (Springer 2008) 115

[43] The aim of restitution is to return parties of the contract to the material position existing prior to the contract. In the situation, where SCs trigger termination of the contract and subsequent restitution by damaging of goods, the general rules of compensation would apply and the seller will merely cover the buyer's damages. See more: Graham Virgo, Restitution in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017)

Chapter 2

In order to answer the liability questions arising from the implementation of the SCs into the ISCG contracts, this chapter elaborates more on the underlying technology. Analysis of this technology is deemed necessary to find out potential flaws of the SCs and instances in which such flaws could trigger civil liability in the context of ISCG contracts. Moreover, this analysis should show potential reasons triggering liability and potential wrongdoers who could be held liable for the flawed performance of SCs in the ISCG contracts.

2.1. The essence of the Blockchain technology

As SCs are powered by the blockchain technology, it is obvious that it could influence the SCs performance.[44] Therefore, it is necessary to figure out whether the blockchain infrastructure could cause misperformance of a SC triggering civil liability and thus whether the creator/owner of the said infrastructure could be held liable. To do so, at least the basics of the blockchain technology should be explained.

At first, though, it is necessary to establish which type of the blockchain is to be analyzed throughout the research. There exist two types of blockchain: permissionless and permissioned.[45] While the former exists in the free computer network without any centralized control, the latter is launched by its creators and exists in the network of the said creators.[46] Since the goals of the SCs implemented into the ISCG contracts is to establish high trust environment without intermediaries, the analyzed blockchain should be permissionless, because it excludes any possibility of the creators' influence on the blockchain execution.[47]

Turning to the explanation of the permissionless blockchain technology, it should be noted that the most outstanding application of the permissionless blockchain came to light with the introduction of the Bitcoin cryptocurrency.[48] Thus, it is easier to show the essence of the permissionless blockchain technology through the Bitcoin example.

Shortly speaking, blockchain is a distributed ledger technology.[49] At its core, the meaning of this for Bitcoin is that data on transactions of cryptocurrency from different accounts is stored simultaneously on multiple computers (nodes) in a system of blocks.[50] Blocks, in their turn, are digital stamps, which contain certain information, including hash code of the previous block, its own hash code generated from the previous hash code and

[44] Vikram Dhillon and others, *Blockchain Enabled Applications* (Apress Berkely 2017) 26

[45] Ying-Ying Hsieh and others, Governance of blockchain-based organizations in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018) 57

[46] Marko Vukolic, 'Rethinking Permissioned Blockchains' [2017] 17(1) Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts 4

[47] Ibid

[48] Ameer Rosik, 'What is Blockchain Technology? A Step-by-Step Guide For Beginners' (BlockGeeks, 18 April 2016) <https://blockgeeks.com/guides/what-is-blockchain-technology/> accessed 5 August 2018

[49] Ibid

[50] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Bitcoin.org*, 1 October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 6 August 2018 1-2

transaction information, time of the stamp, etc.[51] By this information, blocks are chained to each other in a successive position, for each next block contains information about the predecessor block.[52]

In order to establish reliability and authenticity of the information in the blocks and protect it from hacking/exploiting, the verification procedure utilizing encrypted hash codes was introduced.[53] Hash codes are produced by encrypting hash function SHA-256 and represent the encrypted sequences of zeroes and ones, making decryption possible only by guess and check.[54] In essence, each block is created by the addition of the generated hash code from the previous block info and its hash function to the information about transaction itself.[55] Thus, a hash code assigned to the new block is dependent on the data in the previous block, while the latter is predetermined by its predecessor block and so on.[56] That means that any change of any transactional or other data to any of the previous blocks would demand the change of hash codes of all the following blocks in the chain.[57] Though, it could have been easily overcome by hackers and exploiters, if not for the addition of the proof of work [PoW] procedure.

So how does PoW add trust to the blockchain? In course of this procedure, so-called miners (independent members of the system with special computational powers) evaluate special numbers, which in addition to the previous block info would make a hash code for the new block starting with a set number of zeroes.[58] The first miner to guess and check such number adds it to the block info and transfers it to the blockchain. If someone would try to change the previous blocks then the hash codes of the next blocks would change as well and it would be easily noticed as the PoW hash codes would not have the needed number of zeroes in the beginning.[59] In order to overcome this, the potential intruder would have to redo the whole PoW for every block, which would take him an insurmountable amount of computational power, for the intruder would have to guess and check each hash code encrypted by SHA-256.[60]

The above analysis shows that blockchain technology itself is more than protected from any possible kinds of intrusions and is supported by the fact that up to this date there is no evidence of successful blockchain hacking attacks. That, however, does not mean that systems supplementing blockchain could not be hacked (for instance, stock

[51] Ibid 2
[52] Ibid
[53] Ibid 3
[54] Kai Jia and Falin Zhang, Between Liberalization and Prohibition: Prudent Enthusiasm and the Governance of Bitcoin/Blockchain Technology in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018) 166
[55] Nakamoto (n 50) 3
[56] Ibid
[57] Ibid
[58] Nakamoto (n 50) 4; Quinn DuPont, Experiments in Algorithmic Governance: a History and Ethnography of “The DAO” a Failed Decentralized Autonomous Organization in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018) 166
[59] Nakamoto (n 50) 3
[60] Jia and Zhang (n 54) 166

exchanges, stolen private passwords of members, etc.).[61] Nevertheless, as this research is centered at the liability questions in cases where SCs are misperformed these instances are out of concern for the thesis. Thus, there is a low chance of appearance of misperformance of the SCs because of the blockchain infrastructure itself. Consequently, it is highly doubtful that the grounds for the liability claim for the SCs damaging goods may appear in the discussed situation, since there is a low chance of the blockchain to malfunction, or be hacked. Therefore, liability of the infrastructure creators is highly doubtful and will not be further analyzed.

Based on the blockchain technology another important infrastructural element for the SCs exists and is called Ethereum.[62] The main idea of this platform's creator Vitalik Buterin was to allow the high-trust blockchain storing of transactional information to have a further extension in functionality.[63] The latter is achieved through the addition of possibility to implement computer programs into the blockchain.[64] This extends the functions of the blockchain from merely the distributed ledger to the system, which stores and executes computer programs, which are called SCs.[65] For the notion of SCs could have different meanings, it is necessary to provide the analysis of their definition before turning to the further exploration of the Ethereum platform.

2.2. The notion of a SC

The absence of the universal definition of a SC causes a great confusion in the literature, for computer scientists and legal and business community put different meanings into it. Nick Szabo was the first to create the idea of SCs from the legal perspective as a "computerized transaction protocol that executes terms of a contract".[66] In other words, Szabo's initial idea was that SCs would become valuable instruments to help the satisfaction of contractual conditions, but not as contracts from the legal point view. His proposal was amended in 1996 and SCs definition became "a set of promises, specified in digital form, including protocols within which parties perform on these promises".[67] The latter notion changes the meaning of SCs from merely a computer protocol to something resembling a legal contract, for it definitely has some of its characteristics, namely, bilateral or multilateral considerations, two or more parties and definite terms.[68]

Nevertheless, the legal nature of such computer protocols is still under debate. Generally, there are three major legal approaches to SCs: SC as a legal contract, SC as a

[61] Roger A Grimes, 'Hacking bitcoin and blockchain' (CSO, 12 December 2017) <https://www.csoonline.com/article/3241121/cyber-attacks-espionage/hacking-bitcoin-and-blockchain.html> accessed 6 August 2018

[62] Dhillon and others (n 44) 26

[63] Ibid; Rosik (n 48)

[64] Ibid

[65] Dhillon and others (n 44) 27

[66] Nick Szabo, 'Smart Contracts' (Nick Szabo, 1 September) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 6 August 2018

[67] Kristian Lauslahti and others, 'Smart Contracts – How will Blockchain Technology Affect Contractual Practices?'[2017] 1(68) Research Institute of the Finnish Economy Reports 3

[68] Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR) 2009s 1:101(1)

legal action and SC as merely an instrument facilitating legal actions.[69] The first approach is supported by the authors who deem that SCs meet all of the criteria of legal contracts.[70] Apart from those derived from the Szabo's definition of SCs, these authors found out that with certain assumptions SCs are able to give rise to binding legal relationship or have other legal effects (for instance, transfer of assets) and have mutual assent.[71] The second approach considers that either formal legal requirements or inefficiency of SCs as full legal contracts do not allow SCs to be deemed as legal contracts. [72] However, they consider that SCs may have legal effects in some use-cases, which include self-help and escrow.[73]

The additional layer of confusion was created when Vitalik Buterin introduced another meaning of SCs during the reveal of his Ethereum platform.[74] In this iteration SC was merely a complex computer code, which could self-perform on the blockchain infrastructure.[75] Its distinction from other computer programs was that it was recorded on the blockchain, could control blockchain assets itself, and was executed by blockchain infrastructure.[76] Most of its applications had nothing to do with actual legal contracts and, for example, could just store text messages.[77] Thus, SCs in computer science would mean any computation taking place on the blockchain.[78] Accordingly, it could be noted that computer science SCs are the technological basis for SCs in the legal meaning and represent a broader term. Therefore, it is considered reasonable to divide legal aspect of SCs from its computer science counterpart and to name the former as smart contracts [SC] and the latter as smart contract code [SCC].

For the purposes of this thesis the SCs definition is narrowed down to their escrow application, since such working solutions already exist in the ISCG, as described in Chapter 1. Nevertheless, it should be noted that it does not mean that this research limits the analysis exclusively to the escrow functions of the SCs, but deems the inclusion of other options when necessary, though with escrow being the central application of the SC.

2.3. The essence of the Ethereum platform

As it was already mentioned above, Ethereum extended the functionality of the high-trust blockchain mechanisms by allowing the computer code to be used within the

[69] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' [2017] 2017(67) Duke Law Journal; Alexander Savelyev, 'Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law' [2016] 2016(71) Higher School of Economics Research Papers; Max Raskin, 'The Law and Legality of Smart Contracts' [2016] 2017(304) Georgetown Law Technology Review

[70] Werbach and Cornell (n 69) 343; Bill Marino, 'Unpacking the term 'Smart Contract'' (ConsenSys, 10 February 2016) <https://medium.com/@ConsenSys/unpacking-the-term-smart-contract-e63238f7db65> accessed 6 August 2018

[71] Savelyev (n 69) 122-123; Werbach and Cornell (n 69) 333

[72] Raskin (n 69) 322-329

[73] Raskin (n 69) 333; Werbach and Cornell (n 69) 336-338

[74] Marino (n 69)

[75] White paper, 'A Next-Generation Smart Contract and Decentralized Application Platform' (*GitHub*, 1 September 2014) <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 6 August 2018

[76] Josh Stark, 'Making Sense of Blockchain Smart Contracts' (Coindesk, 4 June 2017) <https://www.coindesk.com/making-sense-smart-contracts/> accessed 6 August 2018

[77] Marino (n 69)

[78] Lauslahti and others (n 67) 3-4

platform. This extension, however, could potentially raise security issues of the platform, because the initial philosophy of the blockchain by Satoshi Nakamoto was to limit the functionality of the blockchain, in order to limit the possibility to hack or exploit the system.[79] Conversely, the possibility to code within the system brings the possibility that the users of the system will be able to hack it and thus destroy the high-trust established by the blockchain. Notwithstanding such concerns, the use of the SCCs in Ethereum is considered to be no less safe than the use of the original blockchain for the following reasons.

The establishment of the impenetrable separation between the blockchain infrastructure and the virtual space, in which SCCs are coded and executed, achieves the needed reliability and security.[80] In essence, two virtual spaces are created: the virtual space, where blockchain operates, and the virtual space, where SCCs code is written and stored.[81] The blockchain virtual space remains in its limited functionality, which is in providing transactions between accounts on the blockchain and storing information about these transactions.[82] In order to create an SCC the user should write its code, which is attached to the SCC virtual space, and create the SCC controlled account on the blockchain.[83] After the SCC account is created there is no control over this account by the user, but solely by the SCC, which could send commands to this account to initiate and receive transactions.[84] On the other hand, the SCC is bound to the account on the blockchain and may not be changed or terminated after the creation of such account if only such possibility was not provided in its code.[85] At the same time, transactions to the SCC account in the blockchain virtual space, if they comply with the conditions set in the SCC code stored in the SCC virtual space, trigger certain actions from the SCC.[86] For example, it could be written in the SCC code that the transaction with a certain amount of cryptocurrency (the only possible “currency” in the system) from the SCC account is to be made to another blockchain account after certain conditions are met. These conditions could be limited to the situation when the SCC account receives the transaction of information from yet another blockchain account that the cargo has reached the set geographical location.[87]

From the above description of the Ethereum platform, two ideas may be derived. First, the blockchain limited functional remains, meaning that there is no possibility for the SCC to change the “rules of the game” on the blockchain. This entails the inanity of the exploit and hacking concerns regarding the blockchain infrastructure, because it continues to function as the original blockchain described in the previous paragraph. Second, the SCC after being created acts automatically and may not be changed by anyone. The latter idea establishes trust between the stakeholders in the SCC application,

[79] Dhillon and others (n 44) 26
[80] Ibid, 27
[81] Dhillon and others (n 44) 28, 33-35; DuPont (n 58) 171-172
[82] Ibid
[83] Ibid
[84] Ibid
[85] Ibid
[86] Ibid
[87] IBM, 'Implement your first IoT and blockchain project' (*Watson Internet of Things*, 21 June 2017) <https://www.ibm.com/internet-of-things/platform/private-blockchain/> accessed 5 August 2018; Skuchain.com, 'Brackets' (*Skuchain.com*, 15 November 2017) <http://www.skuchain.com/brackets/> accessed 5 August 2018

since they may be sure that the SCC will act only as prescribed in its code. Therefore, it should be admitted that the chance of the hacking of the Ethereum platform itself is highly doubtful as well as high-trust intrinsic to the original blockchain is provided. Consequently, there are infinitesimal chances that Ethereum could trigger misperformance of the SCs and thus this question is not analyzed further.

Nevertheless, where the problems with the SCCs could occur is on the stage of their coding and following that on the stage of their execution in the SCC virtual space. The fact that SCCs represent computer programs makes them vulnerable to computer bugs during their creation.[88] Bugs in the code could trigger the misperformance of the SCCs and thus the SCs implemented into the ISCG contracts potentially could misperform triggering the liability of the creators of these SCCs for the damage created by this misperformance. In the context of the ISCG industry, either the seller of the goods or a separate company providing SCC development services to the seller could be named among such creators.

Another problem on the same stage of the SCC lifespan may occur with the exploitation of the SCC code as was shown by the DAO “hacking” case.[89] In this case, the vulnerability was figured out in the SCC code establishing a decentralized autonomous organization [DAO].[90] This vulnerability allowed a group of users to withdraw all of the cryptocurrency collected by the DAO members using the functionality provided in the SCC code.[91] At the same time, the blockchain virtual space remained intact and continued to operate normally, meaning that the DAO exploitation was only possible due to the mistakes made in the code of the SCC.[92] Therefore, the liability for not providing sufficient security from hacking or exploitation may be connected solely with the mistakes made during the creation of the SCC by the same actors as in the bug instances.

2.4. Application of the SCs in the context of ISCG industry

Before turning to the analysis of liability triggered by the misperformance of the SC in the ISCG contracts, it is necessary to establish the scenery in which these events these events could take place. For this purpose, IBM Watson SC-IoT and Skuchain solutions to the ISCG industry are described below.

The systems by IBM and Skuchain provide the SCs functional to ISCG contracts, which should establish trust between the parties of the said contract.[93] SCs created for each contract have a number of functions. First, they automatically monitor and control the transportation of goods. This is made through the information sent from the IoT sensors (accounts on the blockchain created for those sensors) dedicated to control the conditions, in which the goods are transported.[94] For instance, these sensors could measure the temperature of the goods, the humidity and pressure rates, etc.[95] Second, SCs

[88] Cem Kaner and others, *Testing Computer Software* (2edn, Wiley 1999) 7
[89] Dhillon and others (n 44) 72-77
[90] Dhillon and others (n 44) 73; DuPont (n 58) 158
[91] Dhillon and others (n 44) 74; DuPont (n 58) 157
[92] Ibid
[93] IBM, 'Implement your first IoT and blockchain project' (n 87); Skuchain.com, 'Brackets' (n 87)
[94] Ibid
[95] Ibid

may control those parameters by operating certain IoT machines installed at the cargo place to maintain the normal conditions of the goods transportation. For instance, they may control the temperature in the refrigerator, etc.[96] Third, these SCs answer for the automatic payment for the delivery of goods.[97] The IoT sensors installed on the goods may track their location and send information to the SCs if the goods reach the destination point. Upon reaching the destination point of the goods, the SC could check whether the goods were transported in the normal conditions from other monitoring sensors and, if this is so, initiate a transaction of payment in the form of cryptocurrency to the seller of goods.[98]

Following this description and the analysis of the SCs technology provided above, certain situations in which misperformance of SCs triggers liability may be named. First, with regard to the monitoring functions of the SCs, the bug in the code of the SC could potentially prevent the SC from receiving the data from the sensors or receiving it in a corrupted manner. This situation may lead to the SC not adequately addressing the deviation of the conditions of goods from normal ending up in their damage or destruction. Moreover, possible exploitation of the SCs by hackers, who hack the sensors and thus provide false information to the SC, could lead to the same situation.

Second, regarding the control functions of the SC, it is possible that the bug in the code leads to the activation of the IoT machines controlling the conditions of goods at a wrong time. This may also lead to the destruction or damaging of the transported goods.

Third, with respect to the location tracker and payment functional of the SCs, the false data from the sensors may lead to the transaction of payment in the situation when the goods are damaged or when the goods have not reached the destination safely. These situations are of no concern for this research, since they are connected with the wrong payment and could be resolved with the application of restitution or unjust enrichment rules.[99]

2.5. Conclusion to Chapter 2

Consequent to everything provided above, a few points could be raised for the further analysis of liability issues connected with misperformance of the SCs, implemented into the ISCG contract. First, the main problem with SCs in the context of ISCG contracts is the possibility of the SCs destroying or damaging the goods. Second, destruction or damaging of goods may take place in two situations: when there is a bug in the SCC code, or when the SC is exploited by hackers. Third, there are different categories of actors who could be held liable for the damaging or destruction of goods in the above situations: seller of the goods, the creator of the SC’s code (could be the seller or a separate entity), the exploiter of the SC.

Nevertheless, for the following reasons exploiters fall out of the scope of this research. First, since in majority of situations it is hard to identify exploiters and hackers,

[96] Ibid

[97] Ibid

[98] Ibid

[99] Graham Virgo, Restitution in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017) 2207

the chance that they will be held liable is low.[100] Second, this chance is further lowered by the fact that pursuing the identified exploiters is not an option for companies.[101] The companies fear reputational losses, confidentiality breaches and subsequent exploits of the same vulnerabilities if the victims report exploiters to authorities.[102] Therefore, there is a low chance that one of the parties of the ISCG contract would sue exploiters and thus exploiters liability is not analyzed in this research.

Using these preliminary conclusions, the next chapter analyses the UK legislation on its suitability as an applicable law in the ISCG contract, implementing the SC-IoT system.

[100] Mary M Calkins, 'They Shoot Trojan Horses Don't They? An Economic Analysis of Anti-Hacking Regulatory Models' [2000] 89(6) Georgetown Law Journal 183; Larry Greenemeier, 'Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers' (Scientific American, 11 June 2011) <https://www.scientificamerican.com/article/tracking-cyber-hackers/> accessed 6 August 2018

[101] Kevin R Pinkney, 'Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure' [2002] 13(3) Albany Law Journal of Science and Technology 63-64

[102] Stevan D Mitchell and Elizabeth A Banker, 'Private Intrusion Response' [1998] 11(2) Harvard Journal of Law & Technology 715; Joginder S Dhillon and Robert L Smith, 'Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques' [2001] 50(1) The Air Force Law Review 145

Chapter 3

It is supposed to be more efficient and demonstrative to study the possible liability issues, which may occur during application of the SC, on an imaginary case as close as possible to the realistic scenario of SCs application. Thus, this chapter building upon the Chapter 2 preliminary conclusions starts with provision of the facts for such a case study and then goes into a detailed analysis of both contract and tort liability issues that may arise between parties of the ISCG contract, using SCs as a tool to ensure performance of their contract.

3.1. Case study facts

For the purpose of the case study, it is assumed that there is a contract of ISCG concluded by two companies from two different countries of origin. They could have chosen any of the jurisdictions as applicable law for their contractual relations, but only UK and FRG law are considered in the case study, for they are the most common jurisdictions generally chosen by the parties of ISCG contracts.[103] The parties also used their right under the Rome II Regulation and chose the same jurisdictions to govern any tort claims derived from their contractual relations.[104] This choice is determined by the desire of the parties to avoid depecage in case the damage of goods by the SC could be both claimed under contract and tort law.[105] USA law, though also being among the most used applicable laws in ISCG, is omitted, as it shows relatively similar approach to UK law in respect of tort and contract liability. While this chapter is limited to the analysis of the liability issues in the context of UK law as applicable law for the contract in question, the next chapter will compare it to the most probable approach of the FRG legislation.

Second, in order to facilitate the analysis of the research question, which could probably be taken by the UK and FRG legislations, the case study is further divided into two situations: a rather simplistic scenario where the seller of goods provides the SC and IoT devices and a more complicated scenario aggravated by third parties intervention. Thus, the facts of the two scenarios are provided below.

According to the first scenario [Case 1], one party sells certain amount of perishable goods to another party for a negotiated sum of cryptocurrency under an ISCG contract with UK law chosen as applicable. It is assumed that the goods are placed into a standard carriage container with IoT systems installed in it and owned by the seller, while their control is executed by a SC coded by the seller.

Parties of the said contract use this SC to transfer the price for the goods automatically when the cargo with goods arrives to the storage of the buyer. This SC also measures certain parameters of the goods throughout their carriage to the buyer (i.e. their temperature, their movement inside the container, etc.) and controls systems to provide

[103] Gilles Cuniberti, 'The International Market for Contracts: The Most Attractive Contract Laws' [2014] 34(3) Northwestern Journal of International Law & Business 459

[104] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the Law Applicable to Non-Contractual Obligations (Rome II) [2007] OJ 2 199/40 s 14(1)(b)

[105] Craig M Gertz, 'The Selection of Choice of Law Provisions in International Commercial Arbitration: A Case for Contractual Depecage' [1991] 12(3) Northwestern Journal of International Law & Business 178-180; Willis LM Reese, 'Dépeçage: A Common Phenomenon in Choice of Law' [1973] 73(1) Columbia Law Review 63-75

safety and sustainability of the goods (for example, moves the goods inside the container, or switches the refrigerator on and off). The parties agree the seller to initiate the SC after the transfer of the price to the SC account by the buyer. The contract is considered void if the transfer of prescribed sum of cryptocurrency does not arrive to the SC account in a set time in order to establish the escrow.

Next, the buyer transfers the negotiated sum of cryptocurrency to the SC account, and the performance of the contract begins. The goods are placed in the container and the latter is sent to the buyer with the IoT systems activated and controlled by a SC. Subsequently, one of the two situations occur: 1) either a bug in the code of the SC activates/does not activate the systems necessary to provide safety of the goods and they end up being damaged, or 2) a hacking of the IoT sensors leads to the exploitation of the SC commanding the IoT devices to damage the goods.

On the other hand, while the second scenario [Case 2] repeats most of the facts of Case 1, it has following *mutatis mutandis* changes. The developer and provider of the SC and IoT is a third party [Provider], but not the seller. Provider could either sell the said system as a product or provide the system in the form of a service to the seller.

Finally, in both scenarios the buyer being discontent with the outcome of the contract tries to recover his losses caused by harm to the goods he bought. Nevertheless, one more preliminary point is to be raised before the beginning of the substantial analysis of the liability issues. This point is connected with the criteria used for the indication whether an analyzed jurisdiction adequately balances the interests of the seller and the buyer with regard to liability. On the one hand, it is considered that the buyer is interested in the normal performance of the SC and ISCG contract as well as in possibility to recover losses in case of the flawed performance of the SC. On the other hand, the seller is also interested in the normal performance of the contract, but also in the possibility to use the benefits provided by the SC application. Taking these interests into account and applying them to the results of the jurisdictions' analysis, the conclusion will be made whether these jurisdictions are suitable as applicable law for the ISCG contract, implementing a SC as a tool of performance.

3.2. Under which conditions may the buyer sue?

Establishing when, how and whom may the buyer sue is necessary to figure out situations where the buyer may sue in different types of claims, but may not succeed in every claim. The latter is needed to find out whether in all possible situations the buyer will be able to recover losses for the damage of goods. Thus, it is considered to be necessary for the research, first, to draw the line between available actions by establishing situations in which these claims will be actionable and, second, describe the possible outcomes of these liability claims.

In case the ISCG contract is subject to the UK jurisdiction, the buyer who suffered losses as a result of the damage of goods by the seller may try to recover these losses either through the contract, tort or bailee liability.[106] Nevertheless, the complexity of the common law actions system may preclude the buyer from claiming damages under more

[106] Simon J Whittaker, The Relationship Between Contract and Tort in H Beale (ed), in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017) 157; Sale of Goods Act 1979 s 20(3)

beneficial rules of contract law if certain variables are taken into account. As provided below, depending on the moments of transfer of ownership over goods and the risk of damaging of the said goods, the buyer will either have a choice of actions between tort, contract or bailment, or will be able to sue only using one of these actions.

These moments could be established by the parties in the contract, which makes it necessary to consider four different options that they have at their disposal.[107] First, it is possible that the contract prescribes that the moment of the transfer of ownership and the moment of transfer of the risk of damaging goods occur at the same time. Then, if the damage of goods takes place before the described moment, the seller remains to be the owner of the goods, and the buyer will be able to sue the seller only under contract liability, since tort liability demands the ownership of the property as a condition to recover losses for its damage.[108]

On the other hand, if damage of goods takes place after the shift of both the risk and ownership, the seller is considered to fulfill his obligations to deliver the goods in normal conditions and quality. The latter structuring of the transfer of risk and ownership is widespread among the buyers, who intend to resell the goods.[109] One of the most important reasons for this is that the ownership over goods is needed for the buyer to effectively use a consignment – a security verifying the ownership of the cargo and providing an opportunity to transfer the said ownership by a mere transfer of this security to the new owner.[110]

In the above situation, even though the seller is considered to fulfill his obligations to deliver the goods in normal conditions and quality, he remains in obligation to the buyer as a bailee of the goods to prevent their damage.[111] The latter situation will formally give a rise to neither contract nor tort claim, but will encompass the buyer with the action out of bailment.[112] The notion of bailment is specific to the common law systems and represents the relationship between the owner of the thing (bailor) and the one who is in real possession of the thing (bailee). Nevertheless, in essence, this situation does not differ from the tort of negligence claim, because bailment claims out of damage of property are decided under the rules of tort.[113]

Two other scenarios include instances in which the parties decide to separate the moments of transfer of ownership and the risk. In the first situation, the risk is transferred before the transfer of ownership and the damage accrues between these two moments.

[107] Anthony G Guest, Sale of Goods in H Beale (ed), Chitty on Contracts (vol 2, 32nd edn, Sweet & Maxwell 2017) 2184; Sale of Goods Act 1979 s 20(1)

[108] Nicholas J McBride and Roderick Bagshaw, *Tort Law* (5 edn, Pearson Education Limited 2015) 168-169; *Scottish & Newcastle International Limited v Othon Ghalanos Limited* [2008] UKHL 11 [45]-[46]; *Leigh and Sillavan Ltd v Aliakmon Shipping Co Ltd* [1985] UKHL 10 [22]-[35]

[109] Dallas Burtraw and Kristen McCormack, 'Consignment Auctions of Free Emissions Allowances under EPA's Clean Power Plan' [2016] dp-16-20 Discussion Papers 7-8; Tao Chen, 'Examining the effectiveness of the simplified air-cargo express consignment clearance system in Taiwan' [2016] 1(12) Journal of Shipping and Trade 3

[110] Peter Schlechtreim and Ingeborg Schwenzer, *Commentary on the UN Convention on the International Sale of Goods* (4 edn, Oxford University Press 2016) 545

[111] Guest, Sale of Goods (n 107) 2185

[112] Ibid

[113] Ewan G McKendrick, Bailment in H Beale (ed), Chitty on Contracts (vol 2, 32nd edn, Sweet & Maxwell 2017) 265-266; *American Express Co v British Airways Board* [1983] 1 WLR 701 709

This occasion will make the seller subject solely to the contract claims, for the ownership of the goods will still remain with the seller.[114] On the other hand, there is another possible situation when the moment of the transfer of ownership precedes the moment of transfer of risk and the damage occurs between these moments. In this case, the buyer will be considered as an owner of the goods, while contractual risks of damage to the goods will still reside on the seller.[115] This means that the buyer may file two different claims: action from the breach of the contract and the action from the bailment. The latter is confirmed by the fact that the seller is granted with possessory rights by the buyer to finish the delivery of the goods.[116]

Overall, this analysis shows that there are two different kinds of claims, which could be used by the buyer: contract and bailment claims. In the following section, these two claims are applied to the conditions set in the case study in order to assess chances of the buyer to successfully recover losses from the damage of goods in the context of the ISCG contract implementing SCs.

3.3. Contract liability

3.3.1. First case study scenario

To claim the contract liability in the Case 1, the buyer should establish the following elements. First, the buyer should show that there was a breach of contract by the seller.[117] Second, it is to be shown that the buyer sustained recoverable loss stemming from the breach.[118] Third, the breach should qualify for the standard of liability.[119] Finally, it is to be analyzed whether there are defences available to the seller excluding or restricting his liability.[120] Below these elements are applied one by one to the conditions set in the Case 1 in order to find out how effectively could the buyer recover losses from the damage of goods.

Regarding the breach of the contract, it is apparent that it is present if the party to the contract does not fulfil either express or implied obligations imposed on this party by the contract. In the case study, the seller could be in breach of the two following obligations: 1) warranty regarding quality of goods,[121] and 2) consideration that delivered goods could be used for the intended purpose.[122] Under this consideration, a violation could be established if the damage to the goods is of such extent that the goods may not be used for the intended purpose.[123] On the other hand, under the said warranty a violation

[114] McBride and Bagshaw (n 108) 168-169; *Scottish & Newcastle International Limited* (n 108) [45]-[46]; *Leigh and Sillavan Ltd* (n 108) [22]-[35]

[115] Whittaker (n 106) 157

[116] Guest, Sale of Goods (n 107) 2184; Sale of Goods Act 1979s 20(1)

[117] David Pearce and Roger Halson, 'Damages for Breach of Contract: Compensation, Restitution, and Vindication' [2008] 28(1) Oxford Journal of Legal Studies 74; Geoffrey H Beale, Damages in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017) 1892

[118] Ibid

[119] Basil Markesinis and others, *The German Law of Contract: A Comparative Treatise* (2 edn, Hart Publishing 2006) 445; Guest, Sale of Goods (n 107) 2114

[120] Anthony G Guest, Exemption Clauses in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017) 1213; *Rutter v Palmer* [1922] 2 KB 87 92

[121] Sale of Goods Act 1979 s 14(2-2F)

[122] Sale of Goods Act 1979 s 14(3); Guest, Sale of Goods (n 107) 2134-2137

[123] Guest, Sale of Goods (n 107) 2139

may be established even if the damage does not preclude the intended use of the goods, but diminishes the quality of the goods below the threshold set in the contract.[124] Since it would depend on the type of goods to figure out the extent of damage needed to qualify for these obligations, it is presumed, for the sake of brevity, that the damage of goods was sufficient.

With respect to the sustained loss criterion, the buyer should show that the loss “naturally flows from the breach of the contract”.[125] Nevertheless, the question of losses and their types is outside of the scope of the research, because they are decided on a case by case basis and do not have a practical importance for establishing whether the buyer will be able to recover losses.[126] Therefore, for the purpose of this research, it is presumed that the buyer claims recoverable losses, which “naturally flow from the breach of the contract”.

Regarding the standard of liability criterion, it should be noted that UK law applies the strict liability doctrine in the case of violation of the abovementioned considerations and warranties.[127] The strict liability doctrine does not need the fault of the wrongdoer to be established and presumes the mere breach of the obligation and loss from it to be sufficient to establish liability.[128] Therefore, the standard of liability criterion is of no concern for the buyer trying to sue the seller in the conditions such as that at the Case 1, because the criteria of breach and loss are qualified as provided above.

It is, though, of much higher importance for the research to consider the fourth criterion of contract liability, which concerns the defences available to the seller, since they could cause complications for the buyer to sue the seller and thus to recover loss. Among such defences, UK law provides the seller with exemption and *force majeure* clauses.[129] Their purpose is to limit or preclude liability for the contract parties in the situations determined in these clauses.[130] Contrary to the continental school of law where *force majeure* is applicable even if not implemented into contract, the specifics of the UK legislation demand this clause as well as exemption clauses to be inserted into the body of the contract in order for *force majeure* exemption to become binding for the parties of the contract.[131] Nevertheless, even though exemption and *force majeure* clauses have no binding nature if not implemented into the contract, it is hard to find any contract without such provisions.[132] As necessarily being part of the contract, those clauses have different effect depending on their formation and their acceptance by the parties to include these clauses in the contract. If drafted correctly, these clauses could exempt the seller from

[124] Sale of Goods Act 1979 s 14(3)

[125] *Farley v. Skinner* [2001] UKHL 49 [44]

[126] Ibid

[127] Markesinis and others (n 119) 445, Guest, Sale of Goods (n 107) 2114

[128] Markesinis and others (n 119) 445, Guest, Sale of Goods (n 107) 2114; William Swadling, The Judicial Construction of Force Majeure Clauses in E Mckendrick (ed), *Force Majeure and Frustration of Contract, 2nd edn* (Informa Law from Routledge 2013) 3; *Grant v Australian Knitting Mills Ltd* [1933] HCA 35 100; *Henry Kendall & Sons v William Lillico & Sons Ltd* [1969] 2 AC 31 56-57

[129] Guest, Exemption Clauses (n 120) 1212

[130] Ibid

[131] Guest, Exemption Clauses (n 120) 1212; Swadling (n 128) 7; Barry Nicholas, Force Majeure in French Law in E Mckendrick (ed), *Force Majeure and Frustration of Contract, 2nd edn* (Informa Law from Routledge 2013) 21

[132] Joni R Paulus and Dirk J Meeuwig, 'Force Majeure - Beyond Boilerplate' [1999] 37(2) Alberta Law Review 302

liability in the situation such as that in the case study. Nevertheless, the proper drafting would be affected by the differences existing between the exemption and *force majeure* clauses, since UK law provides different rules for the application of these clauses.[133] These different rules are clarified below.

The major difference between exemption and force majeure clauses is in their different formation as provided in UK law. On the one hand, exemption clauses could be structured in three typical ways to exclude or limit liability out of which following two could be relevant for the research. The first type of the exemption clauses could exclude certain duties of the party to the contract, so that the breach itself does not take place (ex. the party is not obliged to maintain safety of goods during their transportation).[134] Thus, the contract in the case study could potentially incorporate an exclusion of the duty to protect goods from SC bug/hacking attack. In its turn, second type of the exemption clause could exclude certain liability otherwise attached to the breach of contract (ex. the party is not responsible for damage sustained by goods during their transportation).[135] Therefore, the latter type could possibly be formed in the ISG contract as excluding liability from damage of goods as a result of SC bug / hacking attack.

Nevertheless, these types of exemption clauses have a low chance of being included into the contract for the following reasons. Since under the UK common law framework exemption clauses should be precisely specified or otherwise considered void, these types of exemption clauses would be formulated in a clear and unambiguous way.[136] This formulation in itself would mean that the seller does not bear responsibility for the destruction of the main object of the contract – goods. Thus, it is considered highly unlikely that a party to an ISCG contract, who in majority of situations represents a professional trader, would risk to have such a provision making the whole performance of the contract dependent on a random event. Consequently, as the appearance of such an exemption clause in the ISCG contract is doubtful, the research of the exemption clauses is not further conducted.

On the other hand, *force majeure* clauses are centered on excluding liability from breaches of contract caused by events falling out of control of the parties (ex. the party is not liable for damage sustained by goods as a result of fire).[137] Following this logic, the potential *force majeure* clause for the case study could be formulated as excluding liability for damage of goods as a result of SC malfunction / hacking attack. If compared to the abovementioned second type of the exemption clause, one could find the following difference. While exemption clause exempts the party from the obligation as such, the force majeure renders this obligation as not breached upon the occurrence of certain circumstances.[138] Another significant difference between the two is that formation of the *force majeure* clause is possible in a more generalized way as explained below.[139]

[133] Guest, Exemption Clauses (n 120) 1305; *Fairclough Dodd & Jones v J.H. Vantol Ltd* [1956] 1 WLR 136 143; *Cero Navigation Corp v Jean Lion & Cie* [2000] EWHC 207 213

[134] Guest, Exemption Clauses (n 120) 1212-1213; *Trade and Transport Inc v Iino Kaiun Kaisha Ltd* [1973] 1 WLR 210 230

[135] Ibid

[136] *Seadrill Management Services Ltd v Gazprom* [2010] EWHC1530 (Comm) [184], [217]-[218]; *Air Transworld Ltd v Bombardier Inc* [2012] EWHC 243 (Comm) [15]

[137] Guest, Exemption Clauses (n 120) 1305

[138] Swadling (n 128) 18-19

[139] Guest, Exemption Clauses (n 120) 1305

UK law provides a possibility to formulate the *force majeure* clause in a much more generalized way, for example, by stating that liability is excluded for *any causes* beyond control of the parties.[140] Such a formation is widely spread in contracts, because it provides a flexible way to exclude liability in the events which could not be enumerated by the parties.[141] Thus, implementation and enforcement of such a provision do not necessarily need the inclusion of the reference to the SC bug/hacking attack. Therefore, the generalized formation of the clause allows the seller to sneak the exemption of liability from the SC bug/hacking attack without disclosing to the buyer that there is an intention to be exempted of liability in these events. To prove that this situation could end up in the buyer losing his ability to establish the fourth criterion of the contract liability and thus to recover loss from the damage of goods, it is necessary to apply the criteria for the enforcement of the *force majeure* to the Case 1.

In order to enforce *force majeure*, the events which are claimed to be *force majeure* should meet the following criteria: 1) these events are with what the claiming party was expected to be concerned; 2) these events are beyond control of the claiming party; 3) the events are not known to the party and unavoidable; 4) there were no reasonable steps that the party could have taken to avoid these events.[142]

First, with regard to the bug in the SC, it is considered that it complies with the criterion of what the seller is expected to be concerned with. In essence, this criterion means that the event which is claimed by the party to be *force majeure* should have a connection with this party's obligation under the contract.[143] This was illustrated by an example in one of the cases where the court established such connection between the obligation of the company to deliver the plane in time and the pandemic event, due to which pilots allocated for delivery died.[144] In essence, this example shows that the aforementioned connection was found in the event affecting the contractual obligation of the delivering party, because without these pilots it was impossible for the delivering party to fulfil the delivery duties.

The same connection could be established between the SC bug/hacking attack triggering the damage of goods and the obligation of the seller to deliver goods capable of being used for their purpose and in sufficient quality. Since the delivery of goods in the case study are conducted with the help of the SC, the SC could be considered to be a part of the delivery procedure. Therefore, the event of a bug in the SC code or a hacking attack on the SC affects the abovementioned obligations of the seller by triggering the SC to damage the goods. Therefore, the seller could easily establish the first criterion for the general *force majeure* clause.

The next *force majeure* criterion, which is that the event should be beyond control of the party claiming *force majeure*, is also satisfied in case of the damage of goods as a result of the bug in the SC code or hacking attack. For a SC is nothing more than a computer program, as it was shown in Chapter 2, the natural rules applicable to software

[140] Guest, Exemption Clauses (n 120) 1305; Alan Berg, The Detailed Drafting of a Force Majeure Clause in E Mckendrick (ed), *Force Majeure and Frustration of Contract, 2nd edn* (Informa Law from Routledge 2013) 98

[141] Paulus and Meeuwig (n 132) 302

[142] Guest, Exemption Clauses (n 120) 1305

[143] *Dunavant Enterprises Inc v Olympia Spinning & Weaving Mills Ltd* [2011] 2 Lloyd's Rep. 619 [31]

[144] *Tandrin Aviation Holdings Ltd v Aero Toy Store* [2010] EWHC 40 (Comm) [46]

will be relevant for the SC as well. It follows from a number of researches in the area of the software development that no computer program is free from bugs,[145] meaning that bugs are not created by programmers intentionally or negligently and may appear at any moment. Moreover, it is stated that even the most thorough test for bugs, which is the only reasonable way to find them, may not guarantee the total protection from these flaws.[146] Thus, the seller developing the SC have no possibility to make a fully bug-free software, meaning that the occurrence of the bug leading to the damage of goods is not under control of the seller. Therefore, the bug in the SC software qualifies for the second criterion of the *force majeure*.

On the other hand, the hacking attack also satisfies the second criterion, for the actions of the hacker are beyond the control of the seller. The hacker in this situation is considered to be the third party, whose actions could be seen as an event out of the control of the party to the contract. This could be proved if considering such acknowledged force majeure events as strikes and war.[147] Both of these events consist of actions and omissions of third parties, meaning that third party's actions, on which the party to the contract does not rely, may be seen as an event out of the control of the party to the contract. Therefore, hacking attack, as being an act of the third party, may be considered to be an event out of the control of the seller and thus the hacking attack complies with the second criterion of force majeure.

Following the same factual information about the nature of computer bugs, it is possible to show that the bug in the SC as well as the hacking attack would qualify to the third criterion of the *force majeure*. This criterion is that the force majeure events are not known to the parties and unavoidable. In essence, this means that the parties at the moment of the conclusion of the contract should not know that this event would occur in the future.[148] The mere possibility that this event would occur in the future is not enough to show that the event does not comply with the notion of the force majeure.[149] The risk of this event occurring could be present though.[150] Precisely the same could be said about the SCs bugs and hacking attacks: the parties are aware that there is a possibility that the bug or a hacking attack could occur, but it is not absolutely necessary that they will. Therefore, the bug in the SC code and the hacking attack pass the third criterion of the *force majeure*.

The last criterion of the *force majeure* to be established by the seller, in order to have a strong defence against the claim such as that in the case study, is that there should

[145] Cem Kaner, 'The Ongoing Revolution in Software Testing' (Cem Kaner, 8 December 2004) <http://www.kaner.com/pdfs/TheOngoingRevolution.pdf> accessed 6 August 2018 2-3; Michael C Gemignani, 'Product Liability and Software' [1981] 8(2) Rutgers Computer & Technology Law Journal 191

[146] Patrick T Miyaki, 'Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?' [1992] 8(1) Santa Clara High Technology Law Journal 131

[147] *Zinc Corp v Hirsch* [1916] 1 K.B. 541 549; *B & S Contracts and Design v Victor Green Publications Ltd* [1984] ICR 419 423

[148] *Trade and Transport Inc* (n 134) 224-227

[149] *Hoecheong Products Co Ltd v Cargill Hong Kong Ltd* [1995] 1 W.L.R. 404 408; *Great Elephant Corp v Trafigura Beheer BV* [2014] 1 Lloyd's Rep 1 [31]-[32]

[150] Guest, Exemption Clauses (n 120) 1305

be no reasonable steps left that the party could have taken to avoid the event.[151] The clarification of this criterion in one of the cases states that "the party seeking to rely on [the *force majeure* event] must show that [it] and its consequences could not have been avoided by taking steps which were reasonable in the particular circumstances".[152] However, the precise formulation of reasonableness for this criterion is not provided, further clarifications could be derived from the case law and literature. The courts and literature, which were considering the issues connected with this criterion of the *force majeure*, refer either to negligence or fault on the side of the party claiming *force majeure*.[153] In other words, the courts do not allow the force majeure criteria to be fulfilled, if the event comes as a result of fault of the claiming party or its negligence. Since the established notion of negligence includes the notion of fault, it is considered that the courts, in essence, apply the negligence test to the fourth criterion of the force majeure.[154]

In the context of the case study, the abovementioned means that the seller should show that the bug in the SC code and hacking attack did not occur due to the seller's negligent actions. On the one hand, since the bug may appear in the code only during the coding of the computer program, the seller should establish that he was not negligent when coding the computer program. On the other hand, seller should show that he did not act negligently, when providing security against hacking attacks during the performance of the SC, because the hacking attack may take place only after the implementation of the SC.

According to UK law to show that the actions leading to the damage were not negligent it is necessary to establish that the wrongdoer was compliant with a standard of care imposed on him in this particular situation.[155] For actors with specific skills the standard of care is established on the level of the ordinary skilled person exercising and professing these skills.[156] Therefore, for the seller to show that he was acting according to the standard of care, imposed on him, it is to be established that the ordinary developer of SCs would have taken the same actions during coding of a SC. With regard to the hacking attack, the seller should show that the ordinary company providing security for its computer program systems would have acted the same.

On a regular occasion, to figure out the compliance of the skilled person actions with the actions of the ordinary professional in the same field the court would apply the test established in the *Bolam v Friern Hospital Management Committee* case. This test is formulated as following: "a [professional] is not guilty of negligence if he has acted in accordance with a practice accepted as proper by a responsible body of [professionals] skilled in that particular art".[157] Therefore, the court may seek for the opinion of the

[151] *Fyffes Group Ltd v Reefer Express Lines Pty Ltd* [1996] 2 Lloyd's Rep 171 196; *Great Elephant Corporation* (n 149) [34]

[152] *Bulman & Dickson v Fenwick & Co* [1894] 1 QB 179 185, *B & S Contracts and Design Ltd* (n 147) 431; A Berg (n 140) 90

[153] *Fyffes Group Ltd* (n 151) 196; *Great Elephant Corporation* (n 149) [34]; *Springwell Navigation Corporation v JP Morgan Chase Bank & Ors* [2010] EWCA Civ 1221[209]; Guest, Exemption Clauses (n 120) 1305; Swadling (n 128) 8

[154] McBride and Bagshaw (n 108) 93

[155] Emily Finch and Stefan Fafinski, *Tort Law* (3 edn, Longman 2011) 40

[156] Ibid

[157] *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582 587

professionals in the field of expertize in question in order to establish the standard of care.[158] Apart from that, the court might apply best practices existing in the considered art, for those practices are established by the bodies of professionals in the same art and represent their opinion on how should a professional act in a particular situation.[159]

Regarding the hacking attacks, the approach to provide professional standards and best practices as a ground to establish the standard of care is applicable, because security standards for computer technology systems exist.[160] However, this direct approach is impossible in the Case 1 with regard to the SC bug, because the market of SC development, especially in the domain of the ISCG, has not appeared yet and thus experts in the field have not appeared in mass to provide their opinion on the ways of the maintaining quality during the development of SCs.

Nevertheless, with regard to the SC bug, the court may address this issue by applying the best practices and professional standards established in the software development industry to find out the standard of care for the SC developer.[161] This could be explained by the fact that software developers, in essence, develop the same kind of product, since SCs are also computer programs, as was shown in Chapter 2. However, the number of different approaches to the quality of software in the industry could prevent the court from establishing the proper standard of care.[162] The problem is further accentuated by the fact that the extent of testing of quality of the computer programs differ in each best practice or standard.[163] If following the standard of care test established in the *Bolam v Friern Hospital Management Committee* case, the SC developer will never be considered negligent if only he applies one of these existing best practice approaches, because each of them represents an opinion of a "responsible body of professionals".[164] Consequently, the most beneficial option for the seller would be to apply the least demanding and least expensive quality standard possible, which could have less protection against bugs. In its turn, this will lead to the deterioration of the buyer's position in the ISCG contract, because the delivery of goods would depend on the occurrence of a bug that would have a higher chance to occur with the low quality standards applied by the seller.

This negative situation can not be tackled with the application of the test established in the *Bolitho v City and Hackney Health Authority* case helping to determine the appropriate opinion of a "responsible body of professionals". In this case it was set that the standard of care of a professional may not be established upon the opinion of the body of professionals if it is not "responsible, reasonable and respectable", since this

[158] *Maynard v West Midlands Regional Health Authority* [1984] 1 All ER 635 639; *Bolitho (Deceased) v City and Hackney HA* [1998] A.C. 232 (HL) 238, 241, 243

[159] Michael D Scott, 'Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?' [2008] 67(2) Maryland Law Review 446

[160] Owasp, 'Open Web Application Security Project' (*OWASP*, 22 January 2018) <https://www.owasp.org/index.php/Main_Page> accessed 6 August 2018; Berkley, 'Minimum Security Standards for Electronic Information (MSSEI)' (*Berkley Information Security and Policy,* 23 April 2013) https://security.berkeley.edu/minimum-security-standards-electronic-information accessed 6 August 2018

[161] Scott (n 159) 446

[162] Zador D Kelemen and others, 'A Data Model for Multimodel Process Improvement' [2012] 24(1) Journal of Software Maintenance and Evolution: Research and Practice 896

[163] Ibid

[164] *Bolam* (n 157) 587

opinion is considered by the court to be “not capable of withstanding logical analysis”.[165] These notions were further clarified in the subsequent case law connected with the medical professionals, part of which is of general nature and could be relevant to provide criteria for figuring out a proper opinion of a “body of professionals” in the context of the case study.[166] Below these relevant criteria are addressed in the context of the case study.

First, one of the criteria established that the standard of care may not stem from the opinion of a “responsible body of professionals”, if such “opinion has overlooked that a “clear precaution” to avoid the adverse outcome for the patient was available”.[167] Under such “clear precaution” the court has understood the existing possibility to easily and inexpensively overcome the risk of the adverse outcome.[168] In the context of the case study that would mean that a professional standard or best practice may not create a standard of care for the developer of the SC, if this professional standard or best practice does not include an existing inexpensive and easy way to overcome the possibility of damaging of goods by the SC. The court, however, stressed in this case that such “clear precaution” may arise only if there are no complex technical or controversial matters in question. Since the different professional standards and best practices recommend to conduct different types of testing of the computer programs, it is hard to arrive at a conclusion that the SC development lies outside of the complex technical and controversial matters.[169] Therefore, any of the professional practices and professional standards regarding the establishment of quality of software will be considered as a proper opinion of the “body of professionals” for the purpose of this criterion.

Second, another criterion for the indication of the appropriate opinion states that such opinion should not fail to weight the “comparative risks and benefits of the chosen course of conduct”.[170] The courts have stated that the experts in the “responsible, reasonable or respectable” opinion should turn their minds to the question of comparative risk and benefits and reach a defensible conclusion on the matter.[171] In other words, for the purpose of the case study it would mean that a proper professional standard and/or best practice should weight the benefits of using a specific way of controlling quality of the SC against the risk of the damaging of goods. This, however, is not possible to establish due to the fact that the market of the SCs in the context of the ISCG has not been established yet and thus the existing professional standards and best practices may not include such a comparison of risks and benefits. Therefore, this criterion may not be applied by the court for it will destroy the possibility to establish a standard of care for the seller in the context of the case study.

Following this line of reasoning, the compliance with above criteria show that all of the professional standards and best practices for the provision of quality of software may be considered as an opinion of the “body of professionals” upon which the standard of care of the seller in the context of the case study may be established. Thus, the seller by showing that he applied one of those professional standards or best practices in the course of the drafting of the SC, could establish that he was acting according to the standard of care imposed on him. Consequently, by this it is shown that the seller was not

[165] *Bolitho (Deceased)* (n 158) 232, 241, 243

[166] McBride and Bagshaw (n 108) 270; Rachael Mulheron, 'Trumping Bolam: a critical legal analysis of Bolitho’s “gloss”' [2010] 69(3) Cambridge Law Review 620-635

[167] *French v Thames Valley Strategic HA* [2005] EWHC 459 (QB) [112]

[168] Ibid

[169] Cem Kaner and others, *Testing Computer Software* (2edn, Wiley 1999) 46

[170] *Bolitho (Deceased)* (n 158) 232, 241-242; *Zarb v Odetoyinbo* [2006] EWHC 2880 [84], [100], [106]

[171] Mulheron (n 166) 619

acting negligently in developing the SC, the bug in which triggered the damage of the goods. Absence of negligence on the side of the seller, in its turn, shows that the seller had no other reasonable steps left to avoid the appearance of the bug in the code and the consequential damage of goods. Finally, all the above means that the seller will be claimed negligent and thus not qualifying for the *force majeure* defence only in the situation where he does not apply quality standards for the development of the SC at all. Conversely, by merely using the lowest quality standards in developing SCs the seller is able to show compliance with the last criterion of the force majeure and may apply it as a strong defence against the buyer's claim for the damage of goods.

On the other hand, the existing security standards for the computer systems allow to compare the risks of the systems operating in real life being hacked and the benefits of the security measures applied to these systems.[172] Therefore, the court will not establish the standard of care of the seller by applying the least secure standard and thus the balance between the interests of the seller and the buyer will not be destroyed.

Nevertheless, the situation with the bug in the SC code shows how much the balance of interests is shifted on the side of the seller. On the one hand, the seller enjoys all of the benefits of the SCs and does not risk anything if he merely applies one of the existing professional standards or best practices for ensuring computer program quality. The absence of risk is explained by the fact that after the application of the *force majeure* clause the maximum negative consequence for him, which could entail the damage of goods by the bug in the SC code, could be the restitution in the course of which he will have to return the cryptocurrency paid by the buyer. On the other hand, the buyer risks by entering the ISCG contract with the SC implemented in it, because in case of the damage of goods by the bug in the SC code he will sustain losses connected with the default of the goods delivery. The buyer will not be able to recover these losses. Therefore, with respect to the first case study, it could be stated that UK law does not adequately balance the interests of the seller and the buyer.

3.3.2. Second case study scenario

With regard to the Case 2, in which the SC is provided to the seller by the Provider, certain *mutatis mutandis* changes to the above analysis apply. First, in both situations, where the Provider sells the SC and IoT system to the seller or provides this system as a service, only the seller may be directly sued by the buyer for the damage of goods, because Provider is not bound by the contract between the seller and the buyer.[173]

Second, if the SC and IoT were acquired by the seller as a product, the seller may not be considered to be a professional developer of the SC and thus the negligence for the fourth criterion of the *force majeure* defence should be shown differently. In the situation where the seller is merely an owner of the SC, but not its developer, the seller's ability to control bugs in the SC code changes. For the seller does not have control over the program code and can not establish quality of the program, he could take only one reasonable step to limit the chance of the bug to occur – not to be negligent when using the SC.

To show the absence of negligence in his use of the SC, the seller may apply the test of reasonable foreseeability developed in the *Roe v. Minister of Health (1954)* case.[174] The facts of the case show that medicine injections were made from the ampules, which

[172] Owasp, 'Open Web Application Security Project' (n 160)

[173] Guenter H Treitel, Third Parties in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017) 1509

[174] *Roe v Minister of Health* [1954] EWCA Civ 7 13

were stationed in a special solution.[175] While the ampules were checked by the medical staff of the hospital for cracks, these ampules had invisible cracks letting in the solution, in which the ampules were stored.[176] As a result of the administration of injections from these ampules, in which the said solution mixed with the medicine, people undergoing medical treatment were injured.[177] In this case, the court established that the injury was not reasonably foreseeable, for at the time of the administration of the injection a reasonable person in the position of the medical staff would not have thought that there was a real risk that the claimants would suffer injury, if they were injected with these ampules.[178]

In the case study, the analogy of the *Roe v. Minister of Health (1954)* could be used to show the absence of reasonable foreseeability for the seller of the SC bug occurring. The parallel between the doctors in this case and the seller in the case study may be established, for neither the doctors had sufficient means to check the ampules for cracks, nor the seller, who does not specialize in the development of SCs, had means to check the SC for bugs. At the same time, the bugs and cracks in the ampules are also analogous, since the occurrence of both of them is eventual, and has a risk nature. Therefore, as the facts of both cases resemble each other in their substance, it could be claimed that it is not reasonably foreseeable for a seller that the SC bug would occur. Consequently, the seller did not act negligently during his use of the SC.

Third, in the situation where the seller acquires the SC system through the service, the possibility for the seller to use the *force majeure* defence is under question, because UK law forbids to base the *force majeure* claim on the inability of the third person to fulfil his contractual obligations.[179] In other words, in the situation where there is a contract between A and B, and A can not perform its contractual duties, because its subcontractor C does not fulfil its obligations to A, A does not have a right to claim *force majeure* as a defence against the B's claim for non-performance of the contract.[180] If applying this rule to the case study, the contract of provision of the SC system should be qualified as a subcontract in the course of the ISCG contract, since the services to provide the SC system are used for the performance of the main obligation in the ISCG contract, i.e. delivery of goods.[181] Therefore, it could be established that the non-delivery of the services to provide the SC system may not be considered as a *force majeure* defence and thus the seller does not have *force majeure* defence in the described situation. Consequently, the seller will be held liable in contract, for without the force majeure defence, all of the contract liability criteria are satisfied.

As it could be seen from the analysis of the second case study scenario, the seller receives the strong *force majeure* defence in the situation, where he acquires the SC as a product. That similarly to the first scenario of the case study prevents the buyer from recovering losses for the possible destruction or damage of goods by the SC bug and again shifts the balance of interests against the buyer.

[175] Ibid

[176] Ibid

[177] Ibid

[178] Ibid

[179] *Dunavant Enterprises Inc* (n 143) [32]; *Coastal (Bermuda) Petroleum Co Ltd v VTT Vulcan Petroleum SA* [1993] 1 Lloyd's Rep. 329 332

[180] Guest, Exemption Clauses (n 120) 1308

[181] *Junior Books Ltd v Veitchi Co Ltd* [1982] ABCLR 07/15 [7]

3.3.3. Preliminary conclusion

Overall, the analysis of the contract liability in UK law regarding the SC bug or hacking attack leading to the damage of goods in the ISCG contract shows that the balance of seller's and buyer's interests in such a contract is flawed. In a number of situations, where the bug in the SC code becomes a reason for the damage of goods and the SC is either developed by the seller or merely owned by him, the buyer may lose his contract claim for damages if the seller invokes a *force majeure* defence. Inasmuch, the absence of balance between the interests of the seller and the buyer in the described situations would lead to the failure of the high trust mechanism of the SC, because no trust could be established if an event out of control of the parties could inflict heavy unrecoverable losses to one side exclusively. On the other hand, though, the situations where the hacking attack on the SC system has triggered the damage of goods or where the SC system is acquired by the seller through the contract of provision of services do not raise the issues of balance of interests and thus the SC goal to establish high trust is achieved.

Nevertheless, the parties of the ISCG contract could use following ways to improve the balancing situation. First, the standard of care for the SC developer could be raised by court making it impossible for the seller to shield himself with any existing professional standard. This, however, will not happen before the establishment of the SC market in the ISCG industry, because only then such court cases could appear. Second, it is possible for the parties to cover the damage of goods by the SC bug with the insurance. On the one hand, specifically insuring the event of the bug could be relatively expensive, for this event is new for the insurance market. Nevertheless, with the development of the market the prices should gradually decrease. On the other hand, all-perils insurance covering all risks beyond control of the parties, including SC bugs, in majority of situations does not provide only limited coverage of losses.[182] Moreover, if the number of accidents with SCs will be on a high level, the insurance companies may decide to exclude SC bugs from the insured events leaving the buyer without an option to take an all-perils insurance.[183] Finally, the parties may include an obligation in the contract and subject the development of the SC code to the highest quality standards available. This will increase the standard of care for the seller, who will be exempted from liability only if he follows the highest standards of quality of the SC development. Nevertheless, negotiation of such a provision is highly doubtful, because it entails high costs for the seller, who would prefer not to include it in the contract and will try to block the negotiation of this provision.

Consequently, even if one of these measures take place, the balancing issue and the lack of trust between the parties should disappear. Nevertheless, implementation of these measures is highly doubtful for the aforementioned reasons. This, in its turn, means that UK law does not adequately address the alleged issues and may not be used as an applicable law for the ISCG contract with respect to the contract claims. Nevertheless, as it was pointed above in this chapter, in certain situations the buyer would have the right to claim in bailment. Therefore, for the consistency of the research it is necessary to figure out whether the balancing issues preventing the application of UK law exist in the domain of bailment claims.

[182] Howard Kunreuther and Mark Pauly, 'Force Majeure - Beyond Boilerplate' [2005] 23(4) Journal of Insurance Regulation 7

[183] Ibid 11-12

3.4. Liability of tort and bailment

3.4.1. Differences between bailment and tort claims

Other common law ways to recover losses for the damage of goods, which could be used by the buyer in the case study, include actions out of bailment and tort. By bailment such a relation between two persons is understood when one of them (bailee) keeps the thing (chattel) of another (bailor).[184] According to UK law, in the sale of goods contract bailment relations appear between the seller (bailee) and the buyer (bailor) after the ownership of goods is transferred to the buyer, but the goods remain under control of the seller, for example, when the seller needs to finalize the delivery of the goods to the buyer.[185] Therefore, in such a case the buyer will be able to claim from the seller the liability for damage of goods.

On the other hand, it is not possible to sue in bailment the persons who are not connected by bailment relations. In the context of the case study, among persons not connected by bailment relations with the buyer, the Providers could be named. Instead, UK law provides a possibility to claim in tort if the person owing another person a duty of care breaches it.[186] Thus, the buyer will be able to claim damages in tort from the Providers, if he shows that they have breached a duty of care owed to the buyer. Such a duty of care, though, will not appear before the buyer acquires the ownership over the goods, because before the transfer of goods this duty of care will be owed to the seller as still being the owner of goods.[187]

Even though these two actions have a different nature, the tests for their establishment share a number of similarities, because the bailment claim is derived from tort law.[188] First, in both claims it is necessary to establish a duty of care.[189] By duty of care an obligation to act or not to act owed by one person to another is understood.[190] In the case study that would mean, for example, that due to the contract obligation to deliver goods to the buyer, the seller owes the buyer a duty to keep the goods safe. While it is necessary to establish the duty of care in tort for each distinct case, it is already presumed to exist in the bailment claim, for the bailee owes the bailor the duty of care to keep the latter's chattel safe.[191] Second, both bailment and tort claims are claims in negligence.[192] This means that the breach of the duty of care is established only if the wrongdoer was not acting up to his standard of care when fulfilling his duty of care, or, in other words, was not acting as a reasonable person, concept of which varies depending on the particular situation.[193] Third, in both actions it is necessary to establish the causal link between the breach of the duty of care and the actions of the wrongdoer.[194] Accordingly, the provided test is further used to analyze the possible buyer's bailment and tort claims in their turn.

[184] McKendrick (n 113) 265

[185] Guest, Sale of Goods (n 107) 2185;

[186] McBride and Bagshaw (n 108) 127

[187] McBride and Bagshaw (n 108) 168-169; *Scottish & Newcastle International Ltd* (n 108) [45]-[46]; *Leigh and Sillavan Ltd* (n 108) 809

[188] McKendrick (n 113) 266; *American Express Co* (n 113) 709

[189] McBride and Bagshaw (n 108) 212, 521

[190] Ibid 212

[191] Ibid 521

[192] McKendrick (n 113) 266; *American Express Co* (n 113) 709

[193] McBride and Bagshaw (n 108) 261, 522

[194] Ibid 283

3.4.2. First case study scenario

With regard to the Case 1, after the transfer of ownership over goods, the buyer will be able to claim only in bailment, for the only two actors in this event are the seller and the buyer connected by the bailment relation as explained above. As it was shown in the test, the duty of care is already presumed, i.e. that the seller owes the buyer a duty of care to keep the goods safe. Therefore, it is possible to move to the second element of the test, which is a standard of care criterion. Since this is the SC bug or hacking attack being the reason for the damage of goods and thus the breach of the duty of care to keep the goods safe, the seller should show that, when developing the SC and providing security from the hacking attacks, he acted as a reasonable person.[195] Consequently, the test for reasonableness is the same as the one analyzed in the domain of the contract liability with regard to the fourth criterion of the *force majeure* defence in the first scenario of the case study. For it was shown there that the seller by applying any of the existing standards for establishing quality of the software would be considered as acting reasonably in developing the SC, the same is right for the same test in the bailment claim. The same could be said about the hacking attack, in the situation of which the seller will be called acting reasonably only if using the relative security standard, but not any security standard.

This in itself means that the seller again has a relatively strong defence against the buyers claim and the balance of interests is shifted towards the seller as was explained in the contract section.

3.4.3. Second case study scenario

With respect to the Case 2, the differences in the provision of the SC to the seller by the Provider, i.e. as a product or as a service, will again have impact on the possible buyer's claims. On the one hand, the buyer will only be able to sue the seller of bailment, but not the Provider of tort if the SC is acquired by the seller as a product. While the duty of care in bailment is automatically established as provided above, in tort the duty of care will not be established for the following reason. For the SC bug is a reason to the damage of goods the duty of care owed by the Provider to the buyer should be sought in whether the Provider has taken all the possible actions to prevent the bug from occurring. This duty of care is of a positive nature, i.e. the Provider owes the buyer to act in a certain way, and thus violates his duty by omission.[196] Only in a limited number of cases, the positive duty of care could be established, including such as when the responsibility of the wrongdoer is assumed, when he creates danger, when he is an employer, etc.[197] The most relevant to the situation described in this paragraph is the assumption of responsibility.

Nevertheless, it does not apply to the case, because to assume the responsibility of the wrongdoer a special relationship between him and the damaged party should be established.[198] In other words, it is to be shown that the wrongdoer owes a duty, or that it

[195] McBride and Bagshaw (n 108) 268-269; *Bolitho (Deceased)* (n 158) 232, 241, 243; *Bolam* (n 157) 587

[196] McBride and Bagshaw (n 108) 213-214;

[197] Ibid 229, 233, 239, 243, 245, 246-249;

[198] Ibid 229;

stems from the facts of the case that he was aware of the existence of this duty.[199] For example, this relationship is established when there is a nomination of the wrongdoer by the third party to fulfil certain obligations towards the damaged party.[200] In the situation where the SC is provided as a product to the seller, the Provider has relations only with the seller, but not with the buyer. Moreover, the SC damaging the goods is under the control of the seller after being sold to him by the Provider meaning that the Provider does not know for what purpose his product is used by the seller. Therefore, the special relationship between the buyer and the Provider does not exist and the buyer may not sue the Provider of tort.

Regarding the bailment claim, however, the seller will be able to show that he was acting reasonably, when using the SC, and thus will be able to destroy the bailment claim of the buyer. This may be explained by the fact that when the seller buys the SC system as a product, the same standard of care will be set for the seller as the standard described in the contract section with regard to the fourth criterion of the *force majeure* defence under the same conditions as described in this paragraph. For it was shown there that the seller was acting reasonably when using the SC, the seller will discard the second criterion of the bailment claim and thus may not be claimed liable in tort. Therefore, it is again apparent that the balance of interests is shifted towards the seller, which is considered a negative factor for the application of UK law in the ISCG contract such as that of the case study.

On the other hand, in the situation where the seller acquires the SC in the form of the service, the buyer has the right to sue both the seller and the Provider. With regard to the seller, the bailment claim is available with the duty of care established as provided above. Nevertheless, the standard of care will again create an obstacle for the buyer to prove that the seller is liable in bailment. For the seller is being merely a user of the SC and not a professional developer of it, a general standard of care applies to him as described in the force majeure analysis with regard to the SC acquired as a product. Following this, the general standard of care allows the seller to use the defence established in the *Roe v. Minister of Health (1954)* case. Consequently, the occurrence of the SC bug will be considered as a reasonably unforeseeable event for the seller and he will be exempted of bailment liability.

With regard to the Provider who provides the SC as a service, the buyer may be still unable to win the tort claim. Even if it is possible to establish the assumption of Provider's responsibility, the standard of care imposed on the latter will not differ from one imposed on the seller developing the SC himself. This is so because the Provider will be considered as a professional developer of the SC and, consequently, by applying any existing software quality standard will be able to avoid the negligence in his actions. Therefore, for no negligence will be established in the Provider's actions, the buyer will not be able to sue the Provider in tort. Once again, it is clear that in the situation described above, the balance of interests in the ISCG contract is shifted towards the seller's side. This does not allow claiming UK law as suitable for the applicable law role in the ISCG contract, implementing a SC.

[199] Treitel (n 173) 1509; *Simaan General Contracting Co v Pilkington Glass Ltd (No. 2)* [1988] QB 758 762-763; *White v Jones* [1995] UKHL 5 11; *Junior Books Ltd* (n 181) [4]
[200] Ibid

3.5. Conclusion to Chapter 3

After conducting the analysis of contract, tort and bailment liability under UK law, it is possible to state that in the majority of situations UK law does not adequately balance the interests of the seller and the buyer in the ISCG contract, implementing a SC. With respect to the contract liability, due to the *force majeure* defence, the seller may be exempted from liability, even if he shows that he was applying the minimum quality standard for the development of the SC. The only situation in which the seller is not exempted from liability, is when the seller is held liable for the flawed performance of the SC, provided as a service by the Provider. Moreover, the proposed tweaks to the situation, including raising of the standard of care for the seller as well as insurance, if implemented, are effective to remedy the balance of interests issue. Nevertheless, these tweaks have a low chance of implementation. Consequently, in the domain of contract liability, UK law may not be considered adequate to balance the interests of the buyer and the seller of the ISCG contract, implementing a SC.

With regard to the tort and bailment liability, UK law again does not provide a fair balance between the interests of the seller and the buyer, for in all of the possible permutations, the buyer can not succeed in recovering damages for the damage of goods by the flawed performance of the SC. Therefore, considering contract, tort and bailment liability, it is apparent that UK law may not be considered suitable for the role of applicable law in the ISCG contract, implementing a SC, for UK law shifts the balance of interests between the buyer and the seller to the seller’s side.

Chapter 4

In this chapter, the analysis of the issues brought by the SCs to the ISCG contracts is continued from the perspective of the FRG law in comparison to the UK law. Thus, the case study conditions remain the same, however the applicable law is changed for the law of the FRG. Nevertheless, in order to conduct the consistent analysis of the problem of balance of seller's and buyer's interests it is necessary to figure out all the possible instances when the buyer will or will not be able to recover his losses for the damage of goods. In order to achieve this, before analyzing the substance of the SC problem, it is necessary to figure out when, how and whom will the buyer be able to sue under the conditions of the case study.

4.1. Under which conditions may the buyer sue?

The FRG law differs from the UK legislation in the types of claims which may be brought before the court by the buyer in case of the damage of goods. While the UK legislation provides contractual, tort and *sui generis* claims out of bailment as it was shown in the previous chapter, the FRG law has only the first two options. It should be noted, though, that the absence of the bailment claim does not severely deviate the situation from the one with the UK applicable law, for the differences between tort and bailment are of little practical importance in the context of the research as it will be shown later. Conversely, the commonality between the UK and FRG legal systems is in the fact that certain claims are actionable only under certain circumstances. Thus, the German law perspective on the actionability of claims is analyzed below starting with claims out of the contract breach and then moving to the tort claims.

With regard to the contract claims, similarly to the UK law, German doctrine states that the performance of the contract that is incompliant with its provisions should be deemed as a breach of this contract.[201] Thus, in the event of the damaging of goods by the malfunctioning SC, the goods will be deemed defect and will qualify for the insufficient performance of the contract and its breach.[202] Apparently, though, only the goods damaged during the existence of the obligation to handle them defect-free are deemed as defect. Just like in the UK law, this obligation is ceased after the transfer of the risk of damaging of goods and their ownership to the buyer and the latter is supposed to be a successful performer of his/her contractual obligations, only if the goods were not damaged before such transfer.[203] In the context of international sales of goods, especially when goods are considered to be resold by the buyer, such moment of transfer of risk and ownership would often take place after the handing of the goods over to the carrier.[204] One of the most important reasons for this is that the ownership over goods is needed for the buyer to effectively use a consignment – a security verifying the ownership of the cargo and providing an opportunity to transfer the said ownership by a mere transfer of

[201] Bürgerliches Gesetzbuch [BGB] 1896 ss 280, 323; Basil Markesinis and others, *The German Law of Contract: A Comparative Treatise* (2 edn, Hart Publishing 2006) 379
[202] BGB (n 201) ss 434, 437
[203] BGB (n 201) s 434
[204] BGB (n 201) s 447

this security to the new owner.[205] According to the abovementioned, similarly to UK law, the buyer's contract claim for the damaged goods under applicable law of the FRG would be actionable if the damage of goods takes place before the moment of the transfer of risk.

Conversely, with respect to the tort claims, under German law any person could resort to the tort claim whenever another person violates one of his protected interests, including right to property.[206] As the notion of property is used here, the possibility to claim damages is limited to the events when the person is an owner of that property[207] and in the context of the research – the owner of the goods. Thus, the buyer in case of damage of the goods by the SC will be able to use the tort claim only after the transfer of the ownership of the goods takes place. Nevertheless, he will still be able to sue in tort before the moment of the transfer of risk, but after the transfer of ownership. The latter is possible due to the German rules and doctrine of concurrence of claims allowing the plaintiff to choose either contract or tort claims in case they both have the same claiming ground.[208] The practical conclusion of the abovementioned is that the buyer in the case study will be able to sue only in contract before the transfer of risk and ownership, in either contract or tort after the transfer of ownership but before transfer of risk, and only in tort after the transfer of both the risk and ownership.

Another relevant question connected with actionability of claims is tied to whether the buyer is able to claim damages from the third party, i.e. the Provider of the SC. With respect to the contract claims, the German legislation restricts the possibility to sue in tort the third parties to the contract, i.e. sub-contractors, among which the Providers may be named. This restriction, in essence, is that the main contractor answers for the actions and omissions of his sub-contractors (strict vicarious liability).[209] However, it does not mean that on every occasion the damaged party will not be able to sue the sub-contractors. For there to be a strict vicarious liability excluding the possibility to sue the sub-contractor, his actions or omissions leading to the damage should be performed in the course of the performance of the contract, but not merely on the occasion of the performance of the contract.[210] While the former takes place when the actions and omissions of the sub-contractor lead to the breach of the main contractor's contractual obligations, the latter means that the actions and omissions of the sub-contractor go beyond the scope of the main contract and do not breach it, but violate non-contractual interests of the damaged party, for example, its property interests.[211] Therefore, in the context of the case study the vicarious liability defence will not cover the Provider from the buyer's tort claim if the damage takes place after the transfer of risk of damaging the goods, because, after this

[205] Peter Schlechtreim and Ingeborg Schwenzer, *Commentary on the UN Convention on the International Sale of Goods* (4 edn, Oxford University Press 2016) 545

[206] BGB (n 201) s 823; Basil Markesinis and Hannes Unberath, *The German Law of Torts: a Comparative Treatise* (4 edn, Hart Publishing 2001) 49

[207] Ibid 50; Cees van Dam, *European Tort Law* (2 edn, Oxford University Press 2013) 132

[208] Ruben de Graaf, 'Concurrent Claims in Contract and Tort: A Comparative Perspective' [2017] 2017(4) European Review of Private Law 716-722; H Koziol, *Basic Questions of Tort Law from a Germanic Perspective* (Jan Sramek Verlag 2012) 102

[209] BGB (n 201) s 278; Markesinis and others (n 201) 450; Koziol (n 208) 213-214; Markesinis and Unberath (n 206) 703

[210] Koziol (n 208) 215

[211] Ibid

moment passes, the obligation of the main contract to deliver goods free from defects ceases to exist.[212]

However, this analysis of the possibility to claim the Provider's liability is relevant only to the Provider's distributing the SC as a service. On the one hand, if the SC is provided as a service, the Provider controls the SC's functionality and thus after the transfer of risk of damaging of goods it will be his actions or omissions damaging the goods. On the other hand, if the seller acquires the SC as a product, he controls the SC during its performance and thus these are his actions and omissions to be deemed damaging the goods, but not the actions of the Provider. Therefore, if taking into account the abovementioned, the buyer will be able to sue the Provider in tort, if the SC was provided in the form of a service and only if the damage took place after the transfer of the risk of damaging of goods.

Overall, the preliminary conclusion to this section is that the buyer will be able to sue the seller only in contract before the transfer of risk and ownership, in either contract or tort after the transfer of ownership but before transfer of risk, and only in tort after the transfer of both the risk and ownership. At the same time the buyer will be able to sue the Provider in tort, if the SC was provided in the form of a service and only if the damage took place after the transfer of the risk of damaging of goods. After figuring out when, how and whom the buyer may sue, the research moves to the analysis of the buyer's chances in succeeding in these claims in order to figure out whether FRG law would provide a fair balance between the interests of the seller and the buyer. The next section begins with the buyer's contract claims against the seller.

4.2. Contract liability

4.2.1. First scenario of the case study

Regarding the first scenario of the case study, as already stated above, claims out of contract in the context of the case study may be filed when there is a breach of contract for which the buyer seeks to impose liability on the seller of goods. In doing so, the buyer should show that there was a breach of the contract,[213] while it is the burden of proof of the seller to show that conditions of liability are not satisfied.[214] While the breach of contract is apparent, if the goods arrive defect as a result of their damaging by the SC and IoT equipment before the transfer of risk and ownership of goods, it could be burdensome to establish other conditions of contract liability. Apart from the contract breach among the criteria for the contractual liability, rules of the FRG legislation provide liability for intentional and negligent violations of contractual provisions,[215] which contradicts the UK approach of strict liability standard for contract breaches.[216] In other words, this rule means that the seller will not be subject to contract liability if he manages to prove that the breach of contract was not a result of his intentional or negligent act or omission.

[212] BGB (n 201) s 434

[213] Markesinis and others (n 201) 444, 280 BGB

[214] Markesinis and others (n 201) 446, 280 BGB

[215] BGB (n 201) s 276

[216] Whittaker (n 106) 161

As the difference between intentional and negligent acts and omissions in the FRG civil law is of mere theoretical nature,[217] the negligence is enough to be assessed as a standard of liability for the seller in the context of the case study. By German legislation the latter standard is understood as the ordinary care, which is required in everyday life by human beings.[218] Thus, for the seller to avoid contract liability it is necessary to show that he followed such an ordinary care. German doctrine and case law further develops the standard making it relatively close to the reasonable person standard (*bonus pater familias*), which is prevalent in the common law standard for fault in tort of negligence.[219] In essence, to decide whether actions or omissions of the wrongdoer qualify as negligence his actions and omissions are compared to actions or omissions of other persons of the typical professional knowledge in question put in the same external circumstances,[220] while their personal shortcomings are not taken into account.[221] Under the first scenario of the case study, it would mean that the seller's standard of care is to be derived from other companies developing SCs in the described conditions.

In establishing the standard of care best practices and standards, existing in the area of the development of SCs, could be helpful, for the best practices and standards show what level of quality and security is expected to be provided by the developers.[222] Nevertheless, in contemporary times it is hardly possible to find companies developing SCs as well as standards or best practices in this domain. However, it could be relevant to make a recourse to the companies developing computer software, for SCs, in essence, are computer programs and these companies also face the problems of bugs in their software and have to figure them out in order to achieve smooth performance of their software.[223] The same is relevant for the security standards. Therefore, in order to establish the standard of care for the seller, his actions and omissions should be measured against the existing standards and best practices in the domain of the computer programs development and security.

However, as it was shown in Chapter 3, there is a large variety of different standards and best practices on the computer programs development market. This situation, similarly to what was analyzed in UK law, raises a question of choice of a relevant standard among the present ones to establish a standard of care for the seller. An indication of what the relevant standard should be could be found in the German Supreme Court (*Bundesgerichtshof*) jurisprudence, which influences the application of the legal rules by the lower German courts.[224] In the case BGH NJW 2000, 2812 the *Bundesgerichtshof* was considering a situation in which an IT company under contract provisions was obliged to withdraw data from the corrupted hardware, but failed to do so. In the course of the case it was figured out that it was not objectively impossible to withdraw this data from the hardware, which was shown by the experience of other companies on the same market. Furthermore, it was established that the IT company have not done everything to recover the data from the hard disk.[225] Therefore, the

[217] Markesinis and Unberath (n 206) 83-84
[218] BGB (n 201) s 276; Markesinis and Unberath (n 206) 84
[219] Ibid
[220] Ibid; Dam (n 207) 232; Koziol (n 208) 188-189
[221] Markesinis and Unberath (n 206) 85
[222] Ibid; Dam (n 207) 232; Koziol (n 208) 189
[223] Cem Kaner and others, *Testing Computer Software* (2edn, Wiley 1999) 2-3
[224] Dam (n 207) 75-76
[225] BGH NJW 2000, 2812 (11.4.2000) 7-8

Bundesgerichtshof came to a conclusion that in order to comply with the standard of care the professionals should do everything what is objectively possible according to the knowledge of the professionals in their field of trade. That in itself sets a high standard for the professionals, who under such conditions could be exempted from liability only if they have tried all of the existing means known in the field of their trade in order to fulfil their obligations. In the context of the case study, it would mean that the seller would have to show that in preventing the damage to the goods, i.e. in preventing the occurrence of bugs in the SC and its hacking, he has applied all the means known to the developers of the computer programs.

Since German law does not provide exclusions even for the new professionals in the field,[226] the above decision leads to the necessary application by the seller of, at least, the highest possible standards providing the most thorough analysis of the SCs for bugs and security issues, because they include the most extensive number of measures to be taken. Conversely, the seller will qualify for the standard of care and thus, as provided above, will be considered negligent triggering the contract liability for the damage of goods by the SC. This situation is beneficial for the buyer, for he may be sure that the performance of the ISCG contract is guarded by the high quality of the SC development and security. At the same time, this situation does not significantly hinder the position of the seller, who enjoys the benefits of the SCs application in the ISCG and at the same time may exempt from liability if following the highest standard in the computer programs development domain. Therefore, the interests of the seller and the buyer under the conditions of the first scenario of the case study are balanced. Consequently, German law as applicable law is more beneficial than UK law, because the former does not need additional tweaks, which could be burdensome for the contract parties (ex. insurance), to balance the interests of the parties.

4.2.2. Second scenario of the case study

With regard to the second scenario, not much could be added, due to the fact that, as it was shown in above, the seller bares strict liability for the actions and omissions of his sub-contractors. This entails that the buyer may not sue the Provider in contract, but the seller will bear the same level of liability as if he was acting or omitting to act instead of the Provider. Therefore, the seller will be liable according to the same rules provided in the previous section and to be exempted from liability the seller will have to show that the Provider was using the highest standards for the development of computer programs. This in itself would stimulate the seller to find the Provider applying the highest standards for quality and security of SCs. Consequently, in such situation the interests of the seller and the buyer are balanced and thus German law sufficiently addresses the issue and could be chosen by the parties as applicable in the ISCG contract implementing the SC.

4.3. Tort liability

4.3.1. First scenario of the case study

Turning to the tort liability, it is necessary to recall that the buyer may sue the seller of tort for damage, which occurs only after the transfer of the ownership over the

[226] BGH NJW 2001, 1786 (13.2.2001) 5-6

goods. To do so, the buyer should establish that there was a violation of one of his protected interests by the seller, this violation resulted in damage to the buyer, that the seller was negligent and that there is a causal link between the violation of his protected interests by the seller and the damage.[227] The damage to the protected interest of the buyer is apparent, because the property of the buyer is damaged, i.e. the goods, and German law protects the interest in securing property.[228]

The violation, in its turn, could be established through the theory of the safety duties.[229] According to this theory, every person should take reasonable precautionary measures in order to prevent damage to other persons. Indeed, the case law shows that such precautionary measures should be provided, for example, by the owner of the car locking it in order to prevent a third party from joyriding it and damaging someone else.[230] In addition, safety duties are to be established by the owner of the building to prevent damage from the snow falling from the roof of the building by installing the signs warning the pedestrians, and etc.[231] As it could be seen from these examples, the safety duties are imposed on the persons in different situations, when their possessions may damage third parties. At the same time, the fact that these duties are imposed on persons means that their violation could be only in the form of omission. Therefore, the safety duties theory is applied in the context of the case study due to the fact that the damage to the goods occurs not through the direct actions of the seller, but through his omission to prevent the hacking of the SC or to remove the bugs from the SC's code, which lead to the damage of goods. Consequently, violation of these safety duties may be established if the seller intentionally or negligently does not provide sufficient precautionary measures to prevent damage to the goods.

Turning to the establishment of negligence and sufficiency of precautionary measures, it should be noted that German law applies the common test of the reasonable person in order to establish negligence in both contract and tort liability.[232] Therefore, the test for negligence provided in the previous section is relevant to the second scenario of the case study. Consequently, the seller will be claimed negligent, unless he shows that his precautionary measures were compliant with the highest standards of quality and security of the computer program development.

Nevertheless, the buyer may face hardship with establishing the causal link between the omission of the seller to provide the sufficient precautionary measures and damage to the goods. The reason for this hardship is concealed in the special rule of causation, developed in German law for omissions. This rule sounds as: "an omission is only causal in respect of a result if actions required by duties would certainly have prevented the occurrence of the result".[233] The wording of this formula indicates that the causal link may be established only if it is certain that the precautionary measures would

[227] BGB (n 201) s 823(1); Dam (n 207) 79
[228] Ibid
[229] Dam (n 207) 86-87
[230] BGH VersR 1964, 301 (12.11.1963) 302
[231] BGH NJW 1955, 300 (08.12.1954) 4-5
[232] Joachim E Willi, 'The "Reasonable Man" in United States and German Commercial Law' [1992] 15(1) Comparative Law Yearbook of International Business International 352-353
[233] BGH NJW 1961, 868 (30.01.1961) 6; Raymond R Zimmerman, Damage Caused by Omission in Winiger and others (eds), *Digest of European Tort Law I: Essential Cases on Natural Causation* (Springer Verlag Wien 2007) 104-106

have prevented the occurrence of damage. With respect to the security standards and measures prescribed in them, the causal link may be established, because different counter-hacking measures are directed against certain hacking methods. In other words, it means that if a certain hacking attack on the SC takes place and the seller does not have a measure prescribed in the security standard against this type of attacks, implemented, the causal link will be established, for this security measure is deemed to be sufficient to prevent this type of attack. Conversely, the same may not be stated about the bug in the SC code, for the maximum what the quality standards allow is to test the software for bugs.[234] These tests do not allow to remove all of the bugs or specific types of bugs, but merely could limit their numbers.[235] Therefore, if a certain bug occurs it is impossible to state that the measures existing in the highest quality standards and imposed as a duty on the seller would have certainly removed this bug. Consequently, the causal link between the safety measures imposed on the seller and the damage to the goods may not be established, which entails the exemption of the seller from liability.

This situation means that the seller even without high level quality standards may be exempted from tort liability, since the causal link will never be established between his duty to take precautionary measures due to the nature of the computer bugs and hardship in their indication. Nevertheless, even though the buyer in the event of the SC bug occurrence may not be able to claim liability in tort, the situation does not create imbalance between the interests of the seller and the buyer. Due to the fact that the seller is interested in limiting his liability on the whole period of the ISCG relationships exist between him and the buyer, the seller will have to apply the highest quality standard. This follows from what was shown in the contract liability section, for the exemption of the seller from contract liability will be possible only if the seller applies the highest quality standard during the development of the SC. As it was shown above, the highest standard of quality limits the chance of the occurrence of bugs in the SC and thus the buyer risks less when entering an ISCG contract with the seller.

This again shows that German law adequately addresses the balancing of the seller’s and buyer’s interests and thus is suitable as an applicable law in the ISCG contract implementing the SC. Moreover, German law in this situation is more beneficial for the buyer than UK law, since the seller under German law has an incentive to choose the highest quality standard. At the same time, under UK law, the seller does not have such an incentive and the buyer will have to persuade the seller to negotiate the highest standard into the contract.

Nevertheless, the problem with the application of the highest quality standard may appear under German jurisdiction if the parties negotiate the moment of transfer of the ownership of goods at the moment of the transfer of goods to the carrier. This is due to the fact that the SC’s main functions, which could damage the goods, i.e. tracking and maintaining of the goods conditions, are applied during the carriage of goods. Consequently, if the moment of the transfer of ownership and risk of damaging goods is

[234] Michael D Scott, 'Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?' [2008] 67(2) Maryland Law Review 446-447

[235] Patrick T Miyaki, 'Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?' [1992] 8(1) Santa Clara High Technology Law Journal 131; Cem Kaner, 'The Ongoing Revolution in Software Testing' (Cem Kaner, 8 December 2004) <http://www.kaner.com/pdfs/TheOngoingRevolution.pdf> accessed 6 August 2018 5

set at the moment of the transfer of goods to the carrier, the application of the main functions of the SC will take place only at the time period, when the buyer may only sue for the damage of goods in tort. Therefore, for no contractual liability for the damage of goods will be possible for the seller during the application of the main SC functions, the seller will lose the incentive to apply the highest standard for the development of the SC. Thus, under described conditions and similarly to UK law, German law does not answer the balance of interests issue adequately.

4.3.2. Second case study scenario

Turning to the second case study scenario with respect to the tort liability, it should be reminded that the buyer might sue in tort either the seller or Provider providing the SC as a service. Therefore, the analysis of the tort liability under the second case study scenario begins with the seller's liability and then proceeds to the Provider's liability.

4.3.2.i. Seller's liability

For both the Provider providing the SC as a service and the Provider providing the SC as a product by developing and implementing the SC act under the instructions of the seller, the rules of vicarious liability should be applied to this situation.[236] These rules under tort law, in contrast to the contract law, limit the liability of the person under whose instructions the "servants" were working.[237] Thus the "instructor" is deemed liable for their actions and omissions, unless he shows that either "he was careful in the selection and instruction of his "servants"" or that "the damage or injury would have occurred even if he had fulfilled these duties".[238] In the context of the case study it means that the seller in order to avoid liability will have to show that he was careful in selection and instruction of the Provider, or that the damage to the goods would have occurred even if he had fulfilled these duties.

In the case of the damage of goods, it would be hard for the seller to show that his instructions and supervision were careful, due to the constringent rules established by courts for proving this.[239] On the other hand, the seller may try to show that the SC bug or hacking would have happened even if all of the instructions and supervision were at place as it was shown in the first scenario regarding the establishment of the causal link. Nevertheless, proving that certain measures do not necessarily prevent the damage and proving that the damage will not occur, if the measures are not applied are different substances. Thus, showing that quality testing may only limit the bugs, but not eradicate them completely, will not prove that the damage would have occurred in any event, because certain bugs could be eradicated through this limitation. For it is the seller's burden of proof to show the inevitability of damage,[240] with the factual information about testing, the seller will not be able to prove this and will be liable for actions and omissions

[236] BGB (n 201) s 831; Markesinis and Unberath (n 206) 695

[237] Markesinis and Unberath (n 206) 700; BGB (n 201) s 831

[238] Ibid

[239] BGH VersR 1984, 67 (15.11.1983) 6-7; BGH VersR 1969, 538 (18.2.1969) 3; BGH VersR 1966, 364 (25.01.1966) 7-8

[240] BGB (n 201) s 831; Markesinis and Unberath (n 206) 700

of the Providers as for his own actions and omissions. Therefore, as it was shown in the previous section the seller will be claimed liable in tort.

While UK law does not achieve the fair balance between the interests of the seller and the buyer in the discussed situation, German law is considered adequate for this issue, for it stimulates the seller to seek for the best Provider possible and thus to limit the chances of the SC bug or hacking occurrence.

4.3.2.ii. Provider's liability

Turning to the Provider's liability in the situation when the buyer may sue the former, it should be noted that not much could be added to the above analysis of the tort liability in the first case study scenario, for these situations are identical from the legal perspective. If the buyer sues the Provider, the Provider's SC development, implementation and security maintenance will be assessed as it was made above. For the SC, developed and implemented by the Provider, damages goods, the damage and protected interests criterion of tort liability is satisfied. Next, for the Provider is the creator of the SC, a safety duty to provide precautionary measures from damaging the goods is imposed on him. The extent of the precautionary measures to be established by the Provider equals the measures, which the seller has to show in the first case study scenario, i.e. the highest security and quality standards. This is so, because the same test for negligence is applied to both the seller and the Provider both measured against other professional developers of SCs and computer programs. Finally, similarly to the results of the first case study scenario, it is possible to establish a causal link between the non-implementation of highest security standards and damage of goods, but impossible to establish it between the highest quality standards and the damage of goods. Therefore, the Provider, providing the SC as a service, may be sued by the buyer in tort for the damage of goods resulting from the hacking attack, because of insufficient security measures (not reaching highest security standards), but cannot sue the same Provider for the damage of goods entailed from the occurrence of the bug in the SC code.

This situation is considered adequately addressing the balance of seller's and buyer's interests issue. Even though the buyer may not sue in tort for the damage of goods as a result of the bug in the SC code, it should be noted that for the same damage the buyer may sue the seller as it was shown in the previous section. Therefore, German law is considered suitable as an applicable law for the alleged situation.

4.4. Conclusion to Chapter 4

After conducting the analysis of contract and tort liability under German law, it is possible to state that in majority of situations it adequately addresses the balance of interests between the seller and the buyer in the ISCG contract, implementing a SC. German law allows the buyer to effectively remedy the damage of goods by the SC affected by both hacking attacks and bugs through the effective possibility to sue the seller and the Provider. Even in the situations where the buyer lacks the power to sue the seller or the provider, German law stimulates the seller to choose the highest security and quality standards when developing the SC or to choose the Provider of the SC with such highest standards. Beneficially to the buyer, this altogether mitigates the possibility of hacking attacks and bug occurrence and thus lowers the risk of damaging the goods and, if the highest standards are not applied by the seller, provides the buyer with possibility to recover losses from the damage of goods through the court claim. At the same time, the seller maintains all of the benefits entailed by the application of the SCs. The only balance of interests issue may be connected with the situation where the parties negotiate the moment of the transfer of ownership and risk of damaging goods for the moment of transfer of goods to the carrier. This is due to the fact that the seller in such a situation will not be held liable both in contract and in tort and thus will not be incentivized to choose the highest quality and security standards.

Therefore, the balance of interests issue is considered to be adequately addressed by German law, which could be used by the parties of the ISCG contract as applicable law. At the same time, if comparing German law to UK law, both of them provide sufficient balance of interests regarding the hacking attacks on the SC. However, UK law does not achieve the same balance of interests between the seller and the buyer with respect to the bug in the SC. UK law provides a sufficient balance in the contract liability domain, but only after significant and costly tweaks to the contractual relations of the parties to the ISCG contract, while German law does not need such tweaks. Furthermore, UK law is considered insufficient for providing protection for the buyer in tort claims, while German law does. Finally, UK law does not incentivize the seller to apply the highest quality standards when developing the SC or to choose the Provider applying such standards, while German law does. Therefore, it is considered that German law is more suitable than UK law to be used as an applicable law in the ISCG contract, implementing SCs.

Conclusion

The goal of this research was to find out whether the trust environment between the actors applying SCs could remain in the context of an ISCG contract utilizing SCs as an instrument for its execution. The concerns that this trust environment is not established under the set conditions were raised by the fact that the rules governing liability issues in ISCG could destroy the balance of interests between the seller and the buyer. On the one hand, interests of the seller and business society were considered in the possibility to use the benefits provided by the application of the SC. On the other hand, the buyer's interests were considered in the ability of the buyer to recover losses for the damage of goods in case of the flawed performance of the SC or at least in mitigation of the chances of the occurrence of the flawed performance of the SC. The concern was that the flawed performance of the SCs damaging the goods might leave the buyer without the possibility to recover losses, for the seller has strong contract and tort liability defences allowing him to avoid liability.

The situation was further complicated since ISCG contracts may be subject to different jurisdictions making the balance of interests different depending on the jurisdiction chosen as applicable law. The analysis was limited to the UK and FRG laws for they represent the most commonly used jurisdictions as applicable law for ISCG contracts. These jurisdictions provide ISCG contract parties with the most beneficial conditions. Therefore, if application of SCs within the ISCG contracts subject to the UK or German law provides a fair balance of interests between the contract parties, it will be possible to state that SCs may provide high trust environment in the ISCG contracts. Moreover, comparison of these jurisdictions could help to figure out the better of the two for the role of applicable law in an ISCG contract implementing SCs. Subsequently, it was decided to formulate the thesis question as: whether UK or German law, if at all suitable, better suits the situations where an unintended execution of a SC as a performance instrument in an ISCG contract leads to the damaging of goods?

For answering this question analysis of the technology underlying the SCs was conducted. This analysis helped to find out that the SCs implemented in the ISCG contracts could be used for the tracking of the position of the goods, for monitoring and maintaining the conditions of the goods and for the automated transfer of payment for the delivery of goods. It was further established that these functions of the SCs could lead to the damage of goods, being the main object of the contract, in two situations: if SC's performance is flawed by either a hacking attack or a bug in the code of the SC. Subsequently, two main actors potentially responsible for the flawed performance of the SC were indicated, among whom the seller and the Provider were named. These facts out of the analysis of the technology underlying SCs were used as a source of creation of a case study. This case study represented the potential application of the SCs in the ISCG contract, SCs' potential flawed performance leading to the damage of goods, reasons for such flawed performance and the actors potentially responsible for the flawed performance and subsequent damage of goods.

The UK and German law frameworks were applied later to the facts of the case study in order to figure out whether these jurisdictions could adequately protect and balance the interests of the parties of the ISCG contract, implementing the SC. On the one hand, interests of the seller were considered in the possibility to use the benefits provided by the application of the SC. On the other hand, the buyer's interests were considered in the ability of the buyer to recover his losses for the damage of goods in case of the flawed performance of the SC or at least in mitigation of the chances of the occurrence of the flawed performance of the SC.

With respect to UK law, the analysis of contract liability regarding the bug in the SC, leading to the flawed performance of the SC and consequent damage of goods, showed that this jurisdiction does not provide fair balance between the interests of the seller and the buyer without application of certain tweaks to the contract or to the courts' jurisprudence. Thus, without the tweaks, UK law did not allow the buyer to effectively claim damages for the damage of goods due to the *force majeure* doctrine exempting the seller from liability if only he or his Provider of the SC were using the minimum standard of quality for the development of the SC. At the same time, the buyer was not able to claim contractual liability with respect to the Provider, for the latter was covered from liability by the doctrine of privity of contract.

Conversely, application of the following tweaks to the contract or to the jurisprudence could make UK law sufficient to balance the interests of the seller and the buyer. These tweaks include: 1) the exclusion of the force majeure clause from the ISCG contract by the parties; 2) negotiation of the highest standard for development of the SC; 3) to cover damages with the help of the insurance; 4) raising of the standard of care for the seller and Provider in the courts' jurisprudence. These tweaks allow to either increase the quality of the SC, which would have less bugs and thus there will be less chances that the goods are damaged as a result of the SC's flawed performance, or to cover the losses of the buyer by insurance. If implemented, these tweaks both increase the chances of the buyer to claim losses for the damage of goods and to minimize the risk of the flawed performance to occur. Nevertheless, it was shown that it is hardly possible that these tweaks will be implemented. Therefore, UK law is considered not adequate to balance the interests of the seller and the buyer with regard to the contract liability in case of the flawed performance of the SC entailed by the occurrence of a bug in its code. Conversely, though, the fair balance was provided by UK law with respect to the liability claims out of the damage of goods resulted from the SC performance affected by a hacking attack.

Regarding the bailment and tort liability, it was again established that UK law does not adequately address the balance of seller's and buyer's interests. In all of the analyzed permutations, it was figured out that the buyer either does not have a right to sue the Provider, or may not succeed in claiming damages against the seller or the Provider. This situation shifts the balance of interests to the seller's side, making the buyer the only risking person in the contract. Therefore, it is considered that UK law may not be deemed as adequately addressing the balance of seller's and buyer's interests and thus is not suitable for the applicable law in the ISCG contract, implementing a SC.

On the other hand, German law provides necessary tools to establish a fair balance between the interests of the seller and the buyer. First, in the majority of situations German law allows the buyer to successfully claim damages for the damage of goods under the conditions described in the case study. Second, the German legal framework incentivizes the seller either to apply the highest quality and security standards for development of the SC or to find the Provider of the SC applying such high standards. The latter also helps to cover the instances when the buyer can not succeed in claiming the damages. However, the only flaw of applying German law for the balancing issue, was found, where the parties to the contract negotiate the moment of the transfer of ownership and risk at the moment of the transfer of goods to the carrier. In the abovementioned situation the seller is exempted of liability and has no incentive to include the highest quality and security standards to the development of the SC. Therefore, German law is considered to adequately balance the interests of the seller and the buyer in majority of liability situations in the context of the ISCG contract, implementing a SC.

Consequently, the answer for the main thesis question is that German law, as an applicable law for the ISCG contract, implementing SCs, better addresses liability issues arising from the flawed performance of SCs than UK law.

Bibliography

Books and Journal Articles

Bakucs Z and Ferto I, *The role of trust in contractual relationships* (Warwick University, Coventry, UK 2013)

Beale HG, Damages in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017)

Berg A, The Detailed Drafting of a Force Majeure Clause in E Mckendrick (ed), *Force Majeure and Frustration of Contract, 2nd edn* (Informa Law from Routledge 2013)

Briggs A, *The Conflict of Laws* (3 edn, Oxford University Press 2013)

Burtraw D and McCormack K, 'Consignment Auctions of Free Emissions Allowances under EPA's Clean Power Plan' [2016] dp-16-20 Discussion Papers

Calkins MM, 'They Shoot Trojan Horses Don't They? An Economic Analysis of Anti-Hacking Regulatory Models' [2000] 89(6) Georgetown Law Journal

Campbell-Verduyn M, Introduction in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018)

Chen T, 'Examining the effectiveness of the simplified air-cargo express consignment clearance system in Taiwan' [2016] 1(12) Journal of Shipping and Trade

Cuniberti G, 'The International Market for Contracts: The Most Attractive Contract Laws' [2014] 34(3) Northwestern Journal of International Law & Business

Dam C, *European Tort Law* (2 edn, Oxford University Press 2013)

Davies K and Nathanson H, 'Standard term escrow agreements: the potential pitfalls for depositors and agents alike' [2013] 28(10) Butterworths Journal of International Banking and Financial Law

Deakin S and others, ''Trust' or Law? Towards an Integrated Theory of Contractual Relations between Firms' [1994] 21(3) Journal of Law and Society

Dhillon V and others, *Blockchain Enabled Applications* (Apress Berkely 2017)

Dhillon JS and Smith RL, 'Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques' [2001] 50(1) The Air Force Law Review

DuPont Q, Experiments in Algorithmic Governance: a History and Ethnography of "The DAO" a Failed Decentralized Autonomous Organization in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018)

Eenmaa-Dimitrieva H and Schmidt-Kessen MJ, 'Regulation through code as a safeguard for implementing smart contracts in no-trust environments' [2017] 2017(13) European University Institute Working Paper Law

Emerson RW, 'A Lecture read before the Mechanics' Apprentices' Library Association, Boston' (Ralph Waldo Emerson, 25 January 1841) <https://emersoncentral.com/texts/nature-addresses-lectures/lectures/man-the-reformer/> accessed 3 August 2018

Finch E and Fafinski S, *Tort Law* (3 edn, Longman 2011)

Gemignani MC, 'Product Liability and Software' [1981] 8(2) Rutgers Computer & Technology Law Journal

Gertz CM, 'The Selection of Choice of Law Provisions in International Commercial Arbitration: A Case for Contractual Depecage' [1991] 12(3) Northwestern Journal of International Law & Business

Greenberg ME, 'International Contracts: Problems of Drafting and Interpreting, and the Need for Uniform Judicial Approaches' [1987] 5(2) Boston University International Law Journal

Guest AG, Exemption Clauses in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017)

Guest AG, Sale of Goods in H Beale (ed), Chitty on Contracts (vol 2, 32nd edn, Sweet & Maxwell 2017)

Graaf R, 'Concurrent Claims in Contract and Tort: A Comparative Perspective' [2017] 2017(4) European Review of Private Law

Grote R, Product Liability Under German and European Law. in Wendler and others (eds), *Key Aspects of German Business Law* (Springer 2008)

Hsieh YY and others, Governance of blockchain-based organizations in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018)

Jia K and Zhang F, Between Liberalization and Prohibition: Prudent Enthusiasm and the Governance of Bitcoin/Blockchain Technology in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2018)

Kaner C and others, *Testing Computer Software* (2edn, Wiley 1999)

Kelemen ZD and others, 'A Data Model for Multimodel Process Improvement' [2012] 24(1) Journal of Software Maintenance and Evolution: Research and Practice

Koziol H, *Basic Questions of Tort Law from a Germanic Perspective* (Jan Sramek Verlag 2012)

Kunreuther H and Pauly M, 'Force Majeure - Beyond Boilerplate' [2005] 23(4) Journal of Insurance Regulation

Lauslahti K and others, 'Smart Contracts – How will Blockchain Technology Affect Contractual Practices?'[2017] 1(68) Research Institute of the Finnish Economy Reports

Markesinis B and others, *The German Law of Contract: A Comparative Treatise* (2 edn, Hart Publishing 2006)

Markesinis B and Unberath H, *The German Law of Torts: a Comparative Treatise* (4 edn, Hart Publishing 2001)

McBride NJ and Bagshaw R, *Tort Law* (5 edn, Pearson Education Limited 2015)

McKendrick EG, Bailment in H Beale (ed), Chitty on Contracts (vol 2, 32nd edn, Sweet & Maxwell 2017)

Miyaki PT, 'Computer Software Defects: Should Computer Software Manufacturers Be Held Strictly Liable for Computer Software Defects?' [1992] 8(1) Santa Clara High Technology Law Journal

Mitchell SD and Banker EA, 'Private Intrusion Response' [1998] 11(2) Harvard Journal of Law & Technology

Mulheron R, 'Trumping Bolam: a critical legal analysis of Bolitho's "gloss"' [2010] 69(3) Cambridge Law Review

Nicholas B, Force Majeure in French Law in E Mckendrick (ed), *Force Majeure and Frustration of Contract, 2nd edn* (Informa Law from Routledge 2013)

O'neil PE, 'The Escrow transactional method' [1986] 11(4) Computer Corporation of America Transactions on Database Systems

Paulus JR and Meeuwig DJ, 'Force Majeure - Beyond Boilerplate' [1999] 37(2) Alberta Law Review

Pinkney KR, 'Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure' [2002] 13(3) Albany Law Journal of Science and Technology

Pearce D and Halson R, 'Damages for Breach of Contract: Compensation, Restitution, and Vindication' [2008] 28(1) Oxford Journal of Legal Studies

Raskin M, 'The Law and Legality of Smart Contracts' [2016] 2017(304) Georgetown Law Technology Review

Reese WLM, 'Dépeçage: A Common Phenomenon in Choice of Law' [1973] 73(1) Columbia Law Review

Savelyev A, 'Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law' [2016] 2016(71) Higher School of Economics Research Papers

Schlechtreim P and Schwenzer I, *Commentary on the UN Convention on the International Sale of Goods* (4 edn, Oxford University Press 2016)

Scott MD, 'Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?' [2008] 67(2) Maryland Law Review

Swadling W, The Judicial Construction of Force Majeure Clauses in E Mckendrick (ed), *Force Majeure and Frustration of Contract, 2nd edn* (Informa Law from Routledge 2013)

Treitel GH, Third Parties in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017)

Virgo G, Restitution in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017)

Vukolic M, 'Rethinking Permissioned Blockchains' [2017] 17(1) Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts

Werbach K and Cornell N, ‘Contracts Ex Machina’ [2017] 2017(67) Duke Law Journal

Werbach K, 'Trust, But Verify: Why the Blockchain Needs the Law' [2018] 33(2) Berkley Technology Law Journal

Whittaker SJ, The Relationship Between Contract and Tort in H Beale (ed), in H Beale (ed), Chitty on Contracts (vol 1, 32nd edn, Sweet & Maxwell 2017)

Williamson OE, *The Economic Institutions of Capitalism* (Collier Macmillan Publishers 1985)

Willi JE, 'The "Reasonable Man" in United States and German Commercial Law' [1992] 15(1) Comparative Law Yearbook of International Business International

Zimmerman RR, Damage Caused by Omission in Winiger and others (eds), *Digest of European Tort Law I: Essential Cases on Natural Causation* (Springer Verlag Wien 2007)

Zweigert K and Kötz H, *An Introduction to Comparative Law* (3 edn, Calderon Press 1998)

Legal Acts

Bürgerliches Gesetzbuch 1896

Sale of Goods Act 1979

Consumer Protection Act 1987

Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR) 2009

Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the Law Applicable to Non-Contractual Obligations (Rome II) [2007] OJ 2 199/40

UK Cases

Bulman & Dickson v Fenwick & Co [1894] 1 QB 179

Zinc Corp v Hirsch [1916] 1 K.B. 541

Rutter v Palmer [1922] 2 KB 87

Grant v Australian Knitting Mills Ltd [1933] HCA 35 100

Roe v Minister of Health [1954] EWCA Civ 7

Fairclough Dodd & Jones v J.H. Vantol Ltd [1956] 1 WLR 136

Bolam v Friern Hospital Management Committee [1957] 1 WLR 582

Henry Kendall & Sons v William Lillico & Sons Ltd [1969] 2 AC 31

Trade and Transport Inc v Iino Kaiun Kaisha Ltd [1973] 1 WLR 210

Junior Books Ltd v Veitchi Co Ltd [1982] ABCLR 07/15

American Express Co v British Airways Board [1983] 1 WLR 701

B & S Contracts and Design v Victor Green Publications Ltd [1984] ICR 419

Maynard v West Midlands Regional Health Authority [1984] 1 All ER 635

Leigh and Sillavan Ltd v Aliakmon Shipping Co Ltd [1985] UKHL 10

Simaan General Contracting Co v Pilkington Glass Ltd (No. 2) [1988] QB 758

Coastal (Bermuda) Petroleum Co Ltd v VTT Vulcan Petroleum SA [1993] 1 Lloyd’s Rep. 329

Hoecheong Products Co Ltd v Cargill Hong Kong Ltd [1995] 1 W.L.R. 404

White v Jones [1995] UKHL 5

Fyffes Group Ltd v Reefer Express Lines Pty Ltd [1996] 2 Lloyd's Rep 171

Bolitho (Deceased) v City and Hackney HA [1998] A.C. 232 (HL)

Cero Navigation Corp v Jean Lion & Cie [2000] EWHC 207

Farley v. Skinner [2001] UKHL 49

French v Thames Valley Strategic HA [2005] EWHC 459 (QB)

Zarb v Odetoyinbo [2006] EWHC 2880

Scottish & Newcastle International Limited v Othon Ghalanos Limited [2008] UKHL 11

Seadrill Management Services Ltd v Gazprom [2010] EWHC1530 (Comm)

Springwell Navigation Corporation v JP Morgan Chase Bank & Ors [2010] EWCA Civ 1221

Tandrin Aviation Holdings Ltd v Aero Toy Store [2010] EWHC 40 (Comm)

Dunavant Enterprises Inc v Olympia Spinning & Weaving Mills Ltd [2011] 2 Lloyd's Rep. 619

Air Transworld Ltd v Bombardier Inc [2012] EWHC 243 (Comm)

Great Elephant Corp v Trafigura Beheer BV [2014] 1 Lloyd's Rep 1

FRG Cases

BGH NJW 1955, 300 (08.12.1954)

BGH NJW 1961, 868 (30.01.1961)

BGH VersR 1964, 301 (12.11.1963)

BGH VersR 1966, 364 (25.01.1966)

BGH VersR 1969, 538 (18.2.1969)

BGH VersR 1984, 67 (15.11.1983)

BGH NJW 2000, 2812 (11.4.2000)

BGH NJW 2001, 1786 (13.2.2001)

Blogs

Adlerstein DM, 'Are Smart Contracts Smart? A Critical Look at Basic Blockchain Questions' (Coindesk, 26 June 2017) <https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract/> accessed 5 August 2018

Greenemeier L, 'Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers' (Scientific American, 11 June 2011) <https://www.scientificamerican.com/article/tracking-cyber-hackers/> accessed 6 August 2018

Grimes RA, 'Hacking bitcoin and blockchain' (CSO, 12 December 2017) <https://www.csoonline.com/article/3241121/cyber-attacks-espionage/hacking-bitcoin-and-blockchain.html> accessed 6 August 2018

Marino B, 'Unpacking the term 'Smart Contract'' (ConsenSys, 10 February 2016) <https://medium.com/@ConsenSys/unpacking-the-term-smart-contract-e63238f7db65> accessed 6 August 2018

Naji S, 'Smart Contracts: What Are They and What Do They Mean for International Trade?' (International Law & Practice, 18 December) <http://ncbarblog.com/smart-contracts-what-are-they-and-what-do-they-mean-for-international-trade/> accessed 5 August 2018

Nakamoto S, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Bitcoin.org*, 1 October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 6 August 2018

Rosik A, 'What is Blockchain Technology? A Step-by-Step Guide For Beginners' (BlockGeeks, 18 April 2016) <https://blockgeeks.com/guides/what-is-blockchain-technology/> accessed 5 August 2018

Shrobe H, 'It is possible to design a computer system that can't be hacked' (CNBC, 30 September) <https://www.cnbc.com/2016/09/30/it-is-possible-to-design-a-computer-system-that-cant-be-hacked-commentary.html> accessed 5 August 2018

Skinner C, 'Five Standout Start-Ups Focused Upon Blockchain Trade Finance' (Chris Skinner's Blog, 2017) <http://thefinanser.com/2016/08/fivestandout-start-ups-focused-upon-blockchain-trade-finance.html/> accessed 5 August 2018

Stark J, 'Making Sense of Blockchain Smart Contracts' (Coindesk, 4 June 2017) <https://www.coindesk.com/making-sense-smart-contracts/> accessed 6 August 2018

Szabo N, 'Smart Contracts' (Nick Szabo, 1 September) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 6 August 2018

Internet Sources

Berkley, 'Minimum Security Standards for Electronic Information (MSSEI)' (*Berkley Information Security and Policy*, 23 April 2013) https://security.berkeley.edu/minimum-security-standards-electronic-information accessed 6 August 2018

Gazelle information technologies, 'Supply Chain Shipment Tracking Using Ethereum Blockchain Based Smart Contracts' (*Gazelle Information Technologies*, 14 September 2017) <https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/> accessed 5 August 2018

IBM, 'Implement your first IoT and blockchain project' (*Watson Internet of Things*, 21 June 2017) <https://www.ibm.com/internet-of-things/platform/private-blockchain/> accessed 5 August 2018

Logistics bureau, 'How Blockchain Can Transform the Supply Chain' (*Logistics Bureau*, 15 November 2017) <https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/> accessed 5 August 2018

Owasp, 'Open Web Application Security Project' (*OWASP*, 22 January 2018) <https://www.owasp.org/index.php/Main_Page> accessed 6 August 2018;

Pravo.ru, 'Юридическая матрица: когда наступит время блокчейна' (*Pravoru*, 21 June 2017) <https://pravo.ru/review/view/141356/> accessed 5 August 2018

Skuchain.com, 'Brackets' (*Skuchain.com*, 15 November 2017) <http://www.skuchain.com/brackets/> accessed 5 August 2018

White paper, 'A Next-Generation Smart Contract and Decentralized Application Platform' (*GitHub*, 1 September 2014) <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 6 August 2018

Worldbank, ‘Exports of goods and services (% of GDP)' (*Worldbank.org*, 1 January 2018) <https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS> accessed 5 August 2018

Worldbank, 'Trade (% of GDP)' (*Worldbank.org*, 1 January 2018) <https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS> accessed 5 August 2018