LIABILITY CHALLENGES IN THE BLOCKCHAIN ECOSYSTEM

ELISABETH M. S. FROMMELT

ABSTRACT

The blockchain ecosystem is made up of different actors, who interact with one another in different ways and through different channels. This ecosystem, and the interactions within it, has remained somewhat in the background over the last few years, with the reach of regulation not extending to its shores. With the increasing application of business in the blockchain, the increased use of cryptocurrencies, and the rising interest in tokenization, this legal grey area has come to the forefront more and more. In light of the fact that transactions can be held with anonymous parties, and that this occurs over decentralized systems with no central counterparties, different situations give rise to liability gaps. The paper analyzes three specific scenarios in which these liability gaps arise and considers whether the Civil Code of Liechtenstein provides a basis to solve these problems. It then considers whether the Token and Trusted Technology Service Provider Act (Blockchain Act), which was passed in Liechtenstein, adds a further dimension to solving liability challenges. The Civil Code in fact provides a basis to solve certain scenarios, and the Liechtenstein Blockchain Act further reinforces this, thus establishing greater legal certainty in Liechtenstein. However, certain liability challenges remain, some of which are inherent to the blockchain system itself. Possible solutions proposed include the introduction of legal personality for the blockchain system, usage of a permissioned system or permissioned layers, as well as the introduction of programmed arbitral tribunal.

TABLE OF CONTENTS

INTRODUCTION
I. OUTLINE

Law and technology are two fields that must constantly adapt to one another. In light of the recent blockchain technological revolution, a legal vacuum has been opened, which brings with it unique challenges. While there are many different legal aspects which could be taken into consideration, this paper seeks to identify the liability challenges within the blockchain ecosystem. The interplay between law and technology will first be considered, followed by an introduction to blockchain technology. The focus of the paper will be upon three different scenarios: the first relating to the blockchain system as a whole, the second to smart contracts and legal smart contracts, and the third to transactions using the blockchain system. These scenarios will first be analyzed within the current Liechtenstein civil law basis to see whether there are any liability gaps, or whether liability is identifiable under current law. In light of the Liechtenstein Blockchain Act ("Blockchain Act"), which was passed on January 1, 2020, it will then consider whether the Blockchain Act closes any of the liability gaps not taken into account through the civil law basis. Finally, the paper proposes possible solutions in order to counter the liability challenges in the blockchain ecosystem.

A. Methodology

1. Choice of Liability Focus

Since blockchain technology is characterized by decentralization, it is interesting to postulate as to the role a legal system plays in this universe, and specifically how liability can be introduced. Liability goes to the heart of the problem, for without an accountable party, there cannot be complete trust in the system if an error occurs, as the lack of an accountable party does not allow a means of recourse or enforceability. This mainly becomes the case as transactions become more complex, as they do when they begin to link real world assets with the "online" world. Liability is also an issue that leaders within this field have identified as a very important topic to address.

2. Sources and Data Collection

A review of existing literature was undertaken, as well as an analysis of the existing legal basis and the Blockchain Act. However, as blockchain technology, when considered through the lens of the law, is a more limited field, it was critical to gain understanding through experts in the field. The Blockchain Act, in particular, is a law which has come into being throughout the course of writing this paper. In light of these developments, there is little literature that could be consulted. It was thus vital to discuss the Blockchain Act with leading practitioners in the field, particularly experts of the Government of Liechtenstein themselves who were involved in the creation of the Blockchain Act, as well as members of the working group who drafted the law and helped to shape it. A series of interviews were conducted with experts from a range of sectors, who provided different viewpoints, in order to gain a holistic and comprehensive understanding of the field. Below is a list providing an overview of the interviewees.

1. Clara Billek: Office of Financial Market Innovation for the Government of the Principality of Liechtenstein;

2. Mauro Casellini, Chief Executive Officer of Bitcoin Suisse AG;

3. Virginia Cram-Martos, Project Leader of Blockchain Whitepaper Project and Co-Leader of Internet of Things in Trade Facilitaiton Project at the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and Chief Executive Officer of Triangularity SàRL;

4. Thomas Dünser, Director of the Office for Financial Market Innovation for the Government of the Principality of Liechtenstein;

5. Emmanuelle Ganne, Seniro Analyst at the World Trade Organization;

6. Thomas Feldkircher, Partner and Attorney at Law at Nägele Attorneys at Law LLC;

7. Thomas Nägele, Managing Partner and Attorney at Law at Nagele Attorneys at Law LLC; and

8. Ralph Wanger, Partner and Attorney at Law at Batliner Wanger Batliner Attorneys at Law Ltd.

II. THE ROLE OF LAW IN SOCIETY

Law has different functions within society. It primarily acts as a deterrent, as it attaches credible threats and sanctions to the act of non-compliance.[1] But the law also acts as an enabling force in society. It opens a plethora of possibilities and introduces concepts "by which people can create corporations, make wills, and, especially, form governments."[2] There is no one way in which law can be described, or its function pinpointed, with different schools of thought assigning it different roles. If one considers legal positivism, a legal system is seen as having "its own ground of validity, its own rationality" and characterizes law as a self-sufficient system.[3] From a realist point of view, "law is a value-processing system," whereby it is a subordinate social system within society.[4] Taking on a wider perspective, law is seen in conjunction to society, whereby the two are "coterminous," with law being "an integral part of the structure of society."[5] Under this view, law represents an expression of the values and spirit of a given society. The Natural Law tradition considers law as "the social actualizing of reason," not just considering a given society but transcending all societies.[6] Finally, if one goes beyond society, law can be seen as "a participation in universal order."[7] Allott suggests that the "wonder of law" is the fact that these five perspectives of law should not be seen in isolation but

---

1 FREDERICK SCHAUER, THE FORCE OF LAW 5 (2015).
2 *Id.* at 2.
3 Philip Allot, *The True Function of Law in the International Community*, 5 IND. J. OF GLOB. LEGAL STUD. 391, 413 (1998).
4 *Id.*
5 *Id.* at 397.
6 *Id.*
7 *Id.*

rather viewed as an expression, or rather a fusion, of these different notions. In essence, law "links everyday human behavior to the order of the universe through the self-ordering of society."[8] It combines the past, present, and the future, allowing a society to maintain its past, while also changing its future structure on a vision developed in the present.[9] The law is as much an enabler of change as a solidifier of present values and an upholder of past interests.

Our normative universe is, however, inhabited by morality and social norms. Social norms and morality may guide our behavior, and noncompliance can result in social penalties such as damage to reputation or guilt. However, these sanctions may not be as systematic, severe, or salient, as the sanctions that the law has at its disposal.[10] In this sense, law does not act in isolation. Moral order can be considered in relation to law and is characterized as the "core values and fundamental beliefs which comprise the basic mores of a particular society at a particular time."[11] Through an amalgamation of diverse views, a dominant moral position can emerge, which represents the core moral order. The law may also have a moral content to it that can change over time, causing the law to move in a particular direction. Law and moral order may overlap, but when the two are completely disconnected, there exists a gap. In that case, the law may move closer to the moral order, or vice versa, depending also on the size of the gap.[12]

III. LAW AND TECHNOLOGY

In this constellation, new technologies represent a revolutionary force that seeps into society through different channels. Technological change brings forth different questions regarding "the legitimacy of laws" and the "impacts on community or moral values."[13] Applying this to the idea of the gap, a new technology may align with current views and morals ingrained in society. However, technology can also act as a disruptive force for law. It could cause a shift in society's norms and views, causing a gap between the moral order and the law. The technology could also align with moral conceptions, but the law at that particular point in time may not have a specific regulation in place relating to the new advancement. In this way, technology can have an effect on the gap

---

[8] *Id.* at 398.

[9] *Id.* at 399.

[10] SCHAUER, *supra* note 1, at 1.

[11] Lynn D. Wardle, *The Gap Between Law and Moral Order: An Examination of The Legitimacy of the Supreme Court Abortion Decisions*, 1980 BYU L. Rev. 811, 812 (1980).

[12] *Id.* at 812-813.

[13] GREGORY N. MANDEL, LEGAL EVOLUTION IN RESPONSE TO TECHNOLOGICAL CHANGE 227 (Roger Brownsword, Eloise Scotford & Karen Yeung eds., 2017).

between the moral order and the law, and if the gap is too great, technological regulation may act as a response.

The rate of this response is also critical. If legal change is too slow, it can lead to problems in different areas, for example, in relation to "privacy and other individual rights concerns."[14] Legal change that is too fast can also have negative consequences. It can hamper innovation and disrupt settled expectations.

Different waves of technologies, such as the internet, and their facilitation of further developments, such as e-commerce, have required diverse responses from the law. Mandel illustrates that there are three lessons to be learned from law and the regulation of technology. Firstly, pre-existing legal categories may no longer apply and should thus not be forced to fit with an issue.[15] Secondly, legal decision makers should not let new technologies "distort their legal analysis." Finally, it is not possible to foresee every possible scenario brought forth by new technologies. It is thus important that legal systems continue to evolve and adapt over time.[16]

IV. BLOCKCHAIN REVOLUTION

A. Introduction to Blockchain

There has been "another quiet revolution," namely that of blockchain technology.[17] While the path towards this technology is rooted in different discoveries dating all the way back to the 1970s (such as peer-to-peer networks, public-private key cryptography, and consensus mechanisms), blockchain was introduced as the underlying technology that operated Bitcoin in 2008.[18]

There is no agreement on the definition of blockchain technology. Blockchain is the most commonly known type of distributed ledger technology.[19] A ledger is "an ongoing log of transactions."[20] There are different types of ledger structures. In order to understand the way in which distributed ledger technology functions, one can compare it to a centralized ledger, which is commonly used as a data storage device in finance. Data is stored on a ledger,

---

[14] *Id.* at 226.
[15] *Id.* at 228-229.
[16] *Id.* at 243.
[17] Vinjay Gupta, *A Brief History of Blockchain,* HARV. BUS. REV., FEB. 28, 2017, at 27.
[18] *Id.* at 28.
[19] David Allessie, Maciej Sobolewski, & Lorenzino Vaccari, *Blockchain for Digital Government: An Assessment of Pioneering Implementations in Public Services,* EUR. COMM'N 8 (2019), https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf.
[20] KAREN KILROY, BLOCKCHAIN AS A SERVICE ¶2 (2019).

which is maintained by a trusted administrator, who records asset transfers. While any ledger can be hacked, the centralized ledger poses more risks, for there is not one single data storage point on a distributed ledger. Nodes are connected, storing data at the same time and achieving consensus.[21] A *distributed* ledger allows for a "chronologically ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network."[22] Having a digital record is advantageous if different parties are recording and sharing information.[23] Transactional events, which are stored de-centrally, can be traced back by any participant.[24] It is also important to note that distributed ledger technology addresses the double spending problem, which has traditionally been solved by having central authorities, such as banks, keep track of transactions. Distributed ledger technology allows the transfer of assets to be validated by the whole network, through carefully designed algorithms.[25]

"Blockchain" refers to the way in which data is stored on the ledger.[26] Blockchain technology achieves four objectives: it verifies whether certain events (such as transactions) have occurred, it states in which order these events happened, it ascertains that these events are recorded in an immutable manner, and it establishes that this process takes place without the necessity of a trusted central authority.[27] Blockchain technology is distinctive in that it is a type of ledger in which, instead of being stored individually,[28] value-exchange transactions are grouped into blocks sequentially.[29] Every block has a timestamp, and cryptographic hashes link blocks together, causing each to be chained to the preceding block.[30] By putting together different data points, the content of a block cannot be manipulated without changing the computed hash.[31] This makes the information stored on a blockchain immutable. Each block's header has a cryptographic hash, which is based on the contents of that block as well as the previous block. Data tampering would be visible, since a change in one character of a block would lead to the generation of a different hash for that block, which would not match the original hash. Also, since the

---

21 Douglas A. Arner, Ross P. Buckley & Dirk A. Zetsche, *Blockchain Distributed Ledgers and Liability*, 4 J. DIG. BANKING 298, 300 (2018).

22 Allessie, *supra* note 19.

23 KILROY, *supra* note 20.

24 Allessie, *supra* note 19.

25 *Id.*

26 Arner, *supra* note 21.

27 Oliver Völkel, *Grundlagen der Blockchain-Technologie und virtueller Währungen* (Ger.), *in* BLOCKCHAIN RULES 2 (Christian Piska ed., 2019).

28 Arner, *supra* note 21.

29 Allessie, *supra* note 19.

30 Arner, *supra* note 21.

31 KILROY, *supra* note 20.

next block would have the original hash, there would be a chain reaction that would cause it to break in its entirety.[32]

Blockchain does not use a centralized server; instead, transactions are distributed and validated via a peer-to-peer network. Every participant has a copy of the blockchain system running on its own peer, or node, which can communicate directly with other peers. Transaction requests are then validated and shared in different ways.[33] As a first step, a request is tested against a smart contract, which has predetermined criteria and checks whether those certain criteria are met. The blocks are then broadcast to each peer in the blockchain network and must follow a process referred to as consensus. There are different consensus mechanisms to validate blocks, the most common ones being proof-of-work, proof-of-stake, and proof-of-authority consensus.[34] Common blockchains that underlie cryptocurrencies like Bitcoin, Ether, or Litecoin use proof-of-work consensus mechanisms, wherein complex mathematical problems are solved. [35] The process of solving this puzzle is referred to as "mining."[36] The more computing power one has in such a system, the higher the likelihood that the problem can be solved. Once a solution is actually found, it can easily be verified by other participants.[37] Since this is a distributed process, in which different participants are simultaneously trying to find a solution, more than one node may find a winning hash. Each winning node can then add the proposed block to the network, which can result in a "temporary fork in the blockchain," where nodes add blocks to different branches, depending on which winning node is closest.[38] The protocol ensures that the longest branch, or the one with the most proof-of-work, is included in the blockchain, while others are discarded, thus leading to consistency among nodes.[39] Proof-of-stake algorithms achieve consensus using a participant's stake, or ownership, of a cryptocurrency in a blockchain system. Therefore, instead of spending money buying mining equipment to engage in proof-of-work, money can be invested in buying a cryptocurrency, which is used as a stake to buy "proportionate block creation chances in the blockchain system by becoming a validator."[40] Validators are selected randomly through the algorithm. Finally, proof-of-authority is "based on the predetermined authority of nodes in a network," allowing only those nodes which have authority to

---

32 *Id.*
33 *Id.*
34 *Id.*
35 Völkel, *supra* note 27, at 4.
36 ARATI BALIGA, UNDERSTANDING BLOCKCHAIN CONSENSUS MODELS 6 (2017).
37 Völkel, *supra* note 27, at 4.
38 BALIGA, *supra* note 36, at 6.
39 *Id.*
40 *Id.* at 8.

validate transactions.[41] This can be used within a business using blockchain, in which the identity of participants would be known.[42] Consensus mechanisms establish trust in the accuracy of data because this process is decentralized. As the nodes agree on proposed transactions, this process ensures data integrity, immutability, and consistency. However, it should be noted that in certain situations these criteria are not met. When considering the proof-of-stake consensus mechanism, there can be problems if this occurs on a small-scale, not widely distributed blockchain.[43] That is because the small-scale blockchain is vulnerable to "51% attacks," which means that a mining pool is able to control 51% of the mining power and write its own blocks or fork the blockchain.[44] This concentration seems impossible to achieve in the common blockchain networks.[45]

B. Core Components of Blockchain Technology

In analyzing the functioning of blockchain systems, the core and interrelated components become evident: decentralization, transparency, and immutability. These components work together to foster trust: instead of having a central party managing transactions, these transactions are validated by a number of participants in a transparent manner, as a permanent record is maintained which is accessible to all participants and cannot be tampered with. Blockchain technology is thus characterized as a "trustless" technology.

C. Blockchain Architecture

Different types of blockchain classifications can be made depending on which actors govern the network and the accesses granted to individuals. A blockchain architecture in which anyone who has the right hardware can validate or commit transactions is said to be "permissionless." If only certain nodes can validate or commit transactions, then this is called "permissioned." Furthermore, if "anyone can participate in transacting using the protocol," then the blockchain architecture is "public," whereas if only certain participants can, then it is "private."[46] Drawing on these distinctions, four major blockchain types emerge. The first is a public permissionless blockchain, wherein "everybody can participate in the consensus mechanism of the blockchain," and "everyone in the world with a connection to the internet is able to transact and see the full

---

41 KILROY, *supra* note 20.
42 *Id.*
43 Völkel, *supra* note 27, at 5.
44 BALIGA, *supra* note 36, at 6.
45 Völkel, *supra* note 27, at 5.
46 Allessie, *supra* note 19, at 15.

transaction log."[47] The second is a public permissioned blockchain, which has the same advantage in that anyone with an internet connection can transact and see the transaction log of the blockchain, but only certain nodes can participate in the consensus mechanism. Third, there is a private permissioned blockchain, which places limits on viewings of the transaction log and being able to transact. It must also be noted that in this case there is also an "architect" or "owner" of the blockchain system, giving that party the power to decide on access and on which nodes can participate in the consensus mechanism. Finally, there is a private permissionless blockchain, in which there is a restriction on who can transact and see the transaction log, yet the consensus mechanism is open to everyone.[48]

The archetype chosen depends on considerations of privacy, transparency, security, and speed, concepts which stand in conflict with one another. With a public permissionless blockchain, one would have full transparency, yet the fact that every user or node could verify transactions would make it slower.[49] With a public permissioned blockchain, one would still opt for transparency, since the read access would be open to all nodes, but only a certain group of nodes that have write access would be able to verify transactions. This could be better in terms of speed, but would be detrimental in terms of security, as this process would be entrusted to a smaller group of nodes.[50] The same considerations would apply for the other two types. With a private permissionless blockchain, one would opt for somewhat more privacy and security, while with a private permissioned blockchain, one would opt for privacy and speed.

The types of blockchains go against core elements of the blockchain network. The "peer-to-peer architecture" presumes that all nodes in a system have equal footing in terms of capabilities and responsibilities. This aspect is violated by the reading and writing limitations. The way in which this reading and writing access is administered and enforced can also have an impact on the distributed nature of the system, as this introduces a "hidden element of centrality."[51] The trustworthiness of the environment is also affected, as it shifts from an "unknown number of peers with unknown reliability and trustworthiness" to nodes that could be "evaluated regarding their trustworthiness beforehand in the course of an onboarding process."[52] While this could foster trust, this could also have an opposite effect if taken together

---

47 *Id.* at 16.
48 *Id.*
49 DANIEL DRESCHER, BLOCKCHAIN BASICS: A NON-TECHNICAL INTRODUCTION IN 25 STEPS 214 (2017).
50 *Id.* at 215-16.
51 *Id.* at 217-18.
52 *Id.* at 218.

with the hidden centrality. The individuals making these choices would need to be audited externally in making these choices, for the hidden centrality could cause a certain elite to be chosen, which would be in control of the system.

V. BLOCKCHAIN AND LIABILITY

A. Regulation of Blockchain Technology

Many governments have started to consider, or already devised, legislation which would respond to legal challenges which blockchain technology brings forth. Blockchain technology should not circumvent legal norms and remain unregulated, as this creates various legal gaps. Different issues must be considered, as the components of blockchain clash with various legal principles. For example, transparency and immutability stand in tension with privacy and data protection laws. Immutability specifically does not respect "the right to be forgotten" granted through the General Data Protection Regulation (GDPR).[53]

Core legal questions stem back to liability. Typically, in regulated sectors such as financial services, there is a central counterparty or financial intermediary that is regulated. This party is "accountable and takes responsibility for the provision of the services to all of the other participants through a contractual framework underpinned by the legal and regulatory structures."[54] This could be a central bank which oversees clearing and settlement processes.[55] There is no form of centralization in standard public permissionless blockchain systems. Blockchain technology itself is characterized as a "trustless" technology, by shifting the trust one must have in a person or entity to the "cryptographically verifiable system."[56] In that sense, the system regulates itself, and transactions can be carried out without the need for a central counterparty. However, more complex situations may arise as actors engage more with the system. This is especially the case when the "online world" is linked with the "offline world," for example through the tokenization of assets or the performance of an obligation established through a legal smart contract. When this link is created between the two worlds, the technology itself may not be able to provide the necessary solutions, giving rise to the need for a

---

[53] Arner, *supra* note 21, at 301.

[54] Gordon Myers & John Salmon, *Blockchain and Associated Legal Issues in Emerging Markets*, INT'L FIN. CORP. – WORLD BANK (Feb. 17, 2020), https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F.

[55] *Id.*

[56] Kevin Werbach, *Summary: Blockchain, The Rise of Trustless Trust?*, WHARTON PPI B-SCH. FOR PUB. POL'Y SEMINAR SUMMARIES 1, 1-3 (2019).

central counterparty and a legal system to fall back upon. Consideration must then be given to who is liable for the blockchain system, should an individual claim to be damaged. This is further complicated by the fact that "a decentralized ledger can span multiple locations around the world," making it unclear which laws would apply if a dispute were to arise.[57] Even when considering a transaction that could happen over a public permissionless blockchain, it may not be possible to identify the counterparty to the transaction. Without an identifiable counterparty, assigning liability would be impossible if a problem were to arise. This exemplifies that liability can be considered on different meta-levels: one can look to the blockchain system as a whole, as well as to individual transactions and processes on the blockchain.

B. Liability

As law is conceptualized and materializes differently across jurisdictions, liability would have to be considered differently depending on the jurisdiction. It should also be noted that both civil and criminal liability exist; in this paper, Liechtenstein law will be considered, focusing on liability within the realms of *civil law*. Liechtenstein has a civil law system (as opposed to being a common law country), whose legal foundations consist of a fusion of Austrian and Swiss law.[58] The Austrian Civil Code was declared to be the codified civil law of Liechtenstein in 1812.[59] While there have been modifications over time, it is relevant for this analysis to note that the law relating to liability and damages is based on the Austrian Civil Code.

However, as a starting point, one can consider liability as a concept. This is defined in different ways: the "condition of being liable or answerable by law or equity,"[60] "the fact that someone is legally responsible for something,"[61] or "the responsibility of a person, business, or organization to pay or give up something of value."[62] Liability thus rests upon the presupposition that there are different parties to an action, and in the event that one or more of them are damaged, one is answerable by law. At the core of

---

[57] Myers & Salmon, *supra* note 54, at 2.

[58] Thomas Nigg & Domenik Vogt, *Liechteinstein*, *in* LITIGATION & DISPUTE RESOLUTION 2019 164 (Ted Greeno ed., 8th ed. 2019).

[59] Alexander Besenböck & Jürgen Busch, *Von Mailand bis Czernowity – Die Einführung des österreichischen ABGB, Gesamtstaatsidee und nationaler Partikularismus*, *in* EUROPA UND SEINE REGIONEN 2000 JAHRE RECHTSGESCHICHTE 561 (Andreas Bauer & Karl H. L. Welker eds., 2007).

[60] *Liability*, Oxford English Dictionary, https://oed.com/view/Entry/107804?redirectedFrom=liability#eid (last visited Feb. 15, 2020).

[61] *Liability, n…*, Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/liability (last visited Feb. 15, 2020).

[62] *Id.*

liability is the idea of responsibility and accountability which can be attributed to a party.

C. Liability in the Liechtenstein Civil Code

The Liechtenstein Civil Code[63] describes the different reasons on which to base the attribution of fault. These are split into "Verschuldenshaftung," which is fault-based liability, "Gefährdungshaftung," which is strict liability, and "Eingriffshaftung," which is liability for intervention. The principal cause of action used is fault-based liability.[64] In order to determine whether there is even a case in point for liability, there are four different conditions which must be met.[65]

1. Step 1: Damage

The first step involves determining whether there is a damage. A damage is defined in § 1293 FL-ABGB as "each disadvantage which has been caused to someone's assets, rights or person," wherein "a lost profit which someone hopes to acquire in accordance with the ordinary course of things is different therefrom."[66] A distinction is drawn between pecuniary and non-pecuniary damages. Pecuniary damages have a monetary amount attached to them, whereas non-pecuniary damages cannot be quantified. There is a further distinction drawn relating to pecuniary damages (§§ 1323, 1324 FL-ABGB), as these can be split into "positive damage," whereby asset reduction follows from the destruction of an object of legal protection, and "foregone profit," which is induced through the loss of a commercial opportunity.[67]

2. Step 2: Causality

The second question relates to causality. The behavior has to be *conditio sine qua non*, meaning that the damage would not have occurred were it not for a specific behavior. This may also refer to an inaction, in the sense that the damage was caused by the failure to perform a certain action. However, this is not enough to meet the causality requirement, as there can be a causal link that

---

[63] The analysis is based on sources relating to the Austrian Civil Code. This is because the points relating to liability within the Austrian Civil Code are in most cases analogous to those in Liechtenstein law. When there is a discrepancy, reference will only be made to the Austrian Civil Code as a basis (FL-ABGB versus AT-ABGB).

[64] GEORG KODEK, STEFAN PERNER & MARTIN SPITZER, BÜRGERLICHES RECHT 270 (3rd ed. 2012).

[65] *Id.* at 274.

[66] PETER ESCHIG, DAS ÖSTERREICHISCHE ABGB – THE AUSTRIAN CIVIL CODE 308 (Erika Pircher-Eschig trans., 2013).

[67] KODEK ET AL., *supra* note 64, at 280-81.

would not justify liability. For example, the parents of a damaging party would otherwise be responsible for a damage caused by their child, as this would not have resulted if the damaging party had not been born. Instead, there is a further requirement that the occurrence of the damage should be foreseeable and should not represent an atypical causal event. This limits the *conditio sine qua non,* and only logical occurrences would meet the condition of causality. The following provides an example of this theory: if a hotel employee dropped a suitcase, they would not be expected to foresee the existence of explosives within the suitcase which would lead to an explosion in the hotel, as this is an atypical causal event. Finally, a damage can also be caused by multiple parties, in which case they would all be liable for the entire damage.[68]

3. Step 3: Unlawful Action

The third step to determine liability is referred to as "Rechtswidrigkeit," which translates to "unlawfulness," meaning that an action is against the law. This condition refers to the fact that one has engaged in an unlawful action if a prohibition or legal requirement is infringed, as the individual should have acted differently. As one of the aims of law is behavioral control, the unlawfulness condition focuses on non-compliant behavior instead of a particular outcome.[69]

§ 1295 para. 1 FL-ABGB states that "the damage may have been caused by breach of a contractual obligation or without reference to a contract."[70] "Rechtswidrigkeit" can thus arise either through a breach of contract or tort. When considering a contractual obligation, one must look to the concrete agreement that was entered, whereby "Rechtswidrigkeit" can extend to the breach of a principal or an ancillary obligation. As regards tortious liability, there is "unlawfulness" if the violation of a "protective law" ("Schutzgesetz") – which seeks to prohibit dangerous conduct in the first place – leads to the realization of a threat. The fault itself can be given through the violation of the law. There are also certain absolute rights which have absolute protection. These include personal rights, such as the right to privacy, or rights *in rem* (a "real" right or right in property – "dingliches Recht"). It also must be determined whether the violated norm and the damage are connected.[71] For strict liability this condition falls away.[72]

---

68 *Id.* at 287-89.
69 *Id.* at 293.
70 ESCHIG, *supra* note 66, at 293.
71 KODEK ET AL., *supra* note 64, at 293-94.
72 *Id.* at 337.

4. Step 4: Fault

The final step is referred to as "Verschulden," or fault, in which one considers whether the party causing the damage would have been expected to behave lawfully. While "Rechtswidrigkeit" judges upon the action, "Verschulden" considers the individual.[73] As in the previous step for strict liability, this condition falls away as fault must not be proven. Strict liability considers actions which are dangerous but permissible.[74]

The general burden of proof principle applies wherein the damaged party has to prove that a fault exists. Out of the four elements, fault is oftentimes the hardest to prove. For the breach of contractual obligations, there is a reverse burden of proof.[75] § 1298 FL-ABGB states that "whoever alleges to have been inculpably prevented from performing his contractual or legal obligations has to provide evidence," thereby placing the burden of proof on the damaging party, instead of the damaged party.[76]

D. Legal Consequences

Steps 1-4 provide the starting point, establishing that a claim for damages exists. There are further requirements that one must take into account which shape the way compensation will result. What must first be considered is the principle of compensation, in which the injured party is to be put in a position as though the damage has not occurred. When this is not possible, monetary compensation is given. Another point that must be considered is the statute of limitations which applies to the claims. There is a limitation period of three years, which begins the moment the injured party has knowledge of the incurred damage as well as of the party who caused damage. [77] § 1489 FL-ABGB stipulates that "if the damaged party was not aware of the damage or of the damaging party," then the "right to claim lapses only after thirty years" instead of three years.[78]

It should also be noted that as contractual and tortious liability can lead to unsatisfactory results, there are two further rules which can apply: liability through *culpa in contrahendo*, and liability through a contract which also protects third parties. The former presumes that there is an obligation before a contract is concluded. It is thus assumed that duties of a pre-contractual

---

73 *Id.* at 304.
74 *Id.* at 337.
75 *Id.* at 308.
76 ESCHIG, *supra* note 66, at 309.
77 *Id.* at 274-275.
78 *Id.* at 356.

obligation are breached. The latter principle extends the scope of protection to other parties who are foreseeably affected by a contract's fulfilment.[79]

E. E-Commerce Law

It is also relevant to consider the E-Commerce law (ECG) in Liechtenstein (which implements Directive 2000/31/EC),[80] as this speaks of "provider" liability. The providers are divided into three groups: access providers, host providers, and content providers. Access providers "offer users access to the Internet."[81] Host-providers "offer web-hosting services."[82] Content providers offer content, which can be their own. However, these groups can also overlap, as a provider can offer more than one of these services. The E-Commerce Law only establishes liability for access and host providers, while content providers are governed by the norms in the Civil Code.[83] According to Art. 13 (ECG), access providers are not liable for content if they act as a conduit, meaning that providers do not modify the information, choose who receives the information, and initiate the transmission. The E-Commerce Law further stipulates in Article 16 ECG that host providers are not liable for the information stored at the request of a recipient of the service if a provider "does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent."[84] If these conditions are not met, it further has to be proven that liability arose based on the general Civil Code.[85]

F. Product Liability

As a Member State of the European Economic Area, the European Directive of July 25, 1985, which concerns liability for defective products,[86] applies to Liechtenstein.[87] Before Liechtenstein's membership to the European Economic Area (EEA), it "enacted a products liability statute in full compliance with the EC Directive in the early 1990s," which is the Gesetz über die Produktehaftpflicht (PrHG).[88] The principle purpose of this law is to attribute

---

79 KODEK ET AL., *supra* note 64, at 317-319.
80 Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).
81 Sabine Fehringer, *Austria*, *in* THE INTERNET [2009] – I: LAWS AND REGULATORY REGIMES (Dennis Campbell eds., 2009).
82 *Id.*
83 KODEK ET AL., *supra* note 64, at 335.
84 Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).
85 KODEK ET AL., *supra* note 64, at 335.
86 Council Directive 85/374, 1985 O.J. (L 210/29) 29 (EC).
87 CEES VAN DAAM, EUROPEAN TORT LAW 4 (2nd ed. 2013).
88 Fehringer, *supra* note 81, at AUT-28.

liability to a producer for damages caused by a defective product if the result is i) an individual's injury or death, or ii) damage or destruction of an item of property, which is of a type intended for private use or consumption and which was respectively used by the damaged party for this purpose. The producer is not liable for the damage to the defective product. The "producer" is "the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as its producer" (Art. 2 PrHG; Art. 3 Council Directive 85/374/EEC).[89] "Product" refers to all movables, whether they are incorporated in another movable or immovable, and electricity (Art. 5 PrHG; Art. 2 Council Directive 85/374/EEC).

G. Corporate Liability

The Liechtenstein Person and Companies Act ("Personen- und Gesellschaftsrecht"; PGR) distinguishes natural persons, juridical persons, and companies without legal personality. Through the juridical person, the Act recognizes that a corporation is a distinct legal entity. Juridical persons specifically include the company limited by shares, establishments, foundations, and trusts. Art. 106 PGR states that corporations and corporate bodies, establishments including foundations devoted to a specific object or purpose, all of which are independent, acquire legal personality through incorporation.[90] The Princely Supreme Court of Liechtenstein recognized the purpose of juridical persons in society since they allow corporations to acquire a separate legal personality. However, the Liechtenstein Supreme Court also noted that this leaves room for abuse, in which case this legal personhood must be negated, thus limiting the concept of a corporation's legal personality. When unlawful or economically unreasonable actions are taken, there is recourse to the natural persons behind the legal entity, which are the bearers of rights and obligations. There are different actions that allow for natural persons to seek legal recourse, amongst others the deliberate breaching of contractual obligations, in the event of an infringement of public policy, or through engagement in fraudulent actions.[91]

While there are great differences across jurisdictions, "business corporations have a fundamentally similar set of legal characteristics," which

---

[89] Council Directive 85/374, 1985 O.J. (L 210/29) 29 (EC).

[90] BRYAN JEEVES, LIECHTENSTEIN COMPANY LAW 17 (1992).

[91] Fritz Reichert-Facilides, *Liechtensteinische Rechtsprechung und Literatur zur Durchgriffshaftung*, *in* GEGENWARTSFRAGEN DES LIECHTENSTEINISCHEN PRIVAT- UND WIRTSCHAFTSRECHTS 20 (Benedikt Marxer, Fritz Reichert-Facilides & Anton K. Schnyder eds., 1996).

include legal personality and limited liability.[92] The International Court of Justice also noted that even international law had to recognize corporations' separate legal personality,[93] for "these entities have rights and obligations peculiar to themselves."[94] The basic characteristic of the corporate structure is "that the company alone, through its directors or management acting in its name, can take action in respect of matters that are of corporate character."[95] Corporations, as juridical persons, have their own assets and liabilities, which are separate from those of shareholder's or manager's assets and liabilities, and vice versa. [96] The firm can be characterized as a "nexus of and for contracts," since a corporation serves as a "common counterparty in numerous contracts."[97] The idea of the "limited liability" of the corporation is a "recognition of separate legal existence," wherein "not only contractual obligations but also extra-contractual tort liabilities are subject to the limited liability concept."[98] There is also reverse limited liability, meaning that "a corporation cannot be held liable for a shareholder's obligation."[99] This concept is also recognized in Liechtenstein corporate law.[100] However, when this juridical separation is abused to shield oneself, the recourse taken by injured third parties and courts is referred to as the "piercing of the corporate veil," which disregards the separate legal personality attributed to corporations.[101]

In the discussion of liability, this illustrates that when a corporation takes on legal personhood, it also assumes liability. This liability is not fully "limited," as through the piercing of the corporate veil, the liability can shift back to the responsible persons who breached certain laws or went against certain duties.

---

92 John Armour, Henry Hansmann, Reinier Kraakman & Mariana Pargendler, *Introduction*, *in* THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH, 1 (John Armour et al. eds., 2017).

93 LUCAS BERGKAMP, LIABILITY AND ENVIRONMENT: PRIVATE AND PUBLIC LAW ASPECTS OF CIVIL LIABILITY 320 (2001).

94 Barcelona Traction, Light and Power Company, Limited (Belg. v. Spain), Judgment, 1970 I.C.J. 3, ¶ 39 (Feb. 5).

95 *Id.* ¶ 42.

96 BERGKAMP, *supra* note 93, at 320.

97 *Id.* at 6.

98 *Id.* at 320.

99 *Id.*

100 Reichert-Facilides, *supra* note 91, at 25.

101 Florence Gypens & Erwin Simons, *Corporate Personality – International Perspectives Part I,* DLA PIPER (2018), https://www.dlapiper.com/~/media/files/insights/publications/2018/10/3316259_corporate_veil_brochure_v18_highres_wocm-compressed.pdf (last visited Feb. 16, 2020).

VI. LIABILITY CHALLENGES IN THE BLOCKCHAIN ECOSYSTEM

A. Existing Legal Basis to Solve Liability Challenges

The discussion on liability in Liechtenstein lays the basis for considerations on whether the Civil Code can solve liability challenges in the blockchain ecosystem. In order to do this, specific scenarios are considered at different levels of abstraction. Table 2 outlines these different scenarios, drawing a distinction between whether these relate to the first meta-level or the sub-meta-levels. The first meta-level refers to the blockchain system as a whole, while the sub-meta-levels are less abstract and go into specific scenarios in the blockchain ecosystem. The legal liability basis which could apply to each scenario is also outlined below.

Table 1: Liability Scenarios

Scenario	**Possible Current Legal Liability Basis**
First meta-level: Blockchain system	Provider liability, Producer liability, Developer liability
Sub-meta-level (A): Smart Contracts and Legal Smart Contracts	Civil law, Fault-based liability
Sub-meta-level (B): Transaction over Blockchain System	Property law as a general basis, yet no real liability to be attributed

B. First Meta-level: Blockchain System

1. Finding a Liable Party in the Blockchain Governance Structure

One could first consider the entire blockchain system as a whole. Blockchain technology and the liability challenges introduced are often compared to challenges also faced during the emergence of the Internet. Court rulings, such as that of *Google Spain v. AEPD* before the Court of Justice of the European Union (CJEU),[102] established that a search engine could be held accountable, and distinguished the search engine's activities "from those of the original publisher of the data."[103] The closest similarity that can be drawn to the party accountable in a blockchain system is the system owner on a private blockchain system, who "enables the distribution of data through the

---

[102] Case C-131/12, Google Spain v AEPD, ECLI:EU:C:2014:317 (May 13, 2014).

[103] Myers & Salmon, *supra* note 54, at 5.

blockchain."[104] Yet in a public blockchain system, "there is no one easily held accountable."[105] A blockchain system is run by the participants in the peer-to-peer network, which could be millions of nodes. It would be impossible in that sense to hold a party accountable, as there is not one specific counterparty.

This consideration also has to do with whether there is a "provider," a "producer," or someone who could be considered a provider or producer, in light of the basis given by the E-Commerce Law or Product Liability Act. In terms of product liability, it would depend on how blockchain technology is characterized. With regards to software for example, when software is "considered to be a product, product liability law can attach."[106] One can then extend this idea and consider software developers within public blockchains, who "provide services to the users of that blockchain."[107] While the software "itself is a product, the work that the developers do to maintain and change it is a service."[108]

The E-Commerce Directive itself defines an "information society service" as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"[109] (In Liechtenstein then, Art. 3 ECG: "jeder in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellte Dienst"). From this point of view, a "blockchain service could consist of a service built upon the blockchain (e.g. smart contracts, storage, etc.), or the provision of the blockchain itself."[110] Whether one considers a blockchain service, or the blockchain itself, it could thus possibly be considered a "service" under the E-Commerce Law.

Identifying participants in the blockchain system is, however, also a challenge. The three distinct groups are represented by miners, nodes, and users. Miners "assemble blockchain transactions in blocks," adding "blocks to the blockchain."[111] Nodes "store a local copy of the blockchain."[112] Users then perform transactions "which are added to the blockchain."[113] It is considered

---

104 *Id.*

105 *Id.*

106 Liis Vihul, *The Liability of Software Manufacturers for Defective Products*, THE TALLINN PAPERS (2014) https://ccdcoe.org/uploads/2018/10/TP_02.pdf (last visited Feb. 18, 2020).

107 Angela Walch, *In code(rs) We Trust – Software Developers as Fiduciaries n Public Blockchains*, Regulating Blockchain: Techno-Social and Legal Challenges, 65 (2019).

108 *Id.*

109 Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).

110 Jessica Schoers, *Can blockchain participants use the e-Commerce Directive's liability exemptions?,* UNIV. OF LEUVEN (Mar. 9, 2019) https://www.law.kuleuven.be/citip/blog/can-blockchain-participants-use-the-e-commerce-directives-liability-exemptions/.

111 *Id.*

112 *Id.*

113 *Id.*

that miners could, for example, "have to comply with the intermediary liability specifications under the E-Commerce Directive."[114] Nodes store information, so under the E-Commerce Law, they would need to be able to immediately remove any information once they were aware of any illegal activity. This stands in contrast to the immutable characteristic of blockchain technology.[115]

The examples provided serve to show that different actors could be identified within the blockchain system, which could be subject to existing regulation. However, these are still mere actors within this realm performing functions which would fall into specific liability domains. For example, in the context of the E-Commerce Law, this would be geared towards identifying illegal activity and holding a party accountable in this respect. However, this does not speak to the blockchain system as a whole. Even if one were to subject these actors to the law, this would affect a certain point within the bigger picture. When looking at it in the light of those specific pieces of legislation, there would be no regulation of the system as a whole, or the identification of a single party to assign liability to if there were a problem with the entire blockchain system.

A further group to consider are the "core developer groups that decide on software updates," as they are not just "technology designers but also policy-makers shaping the world we live in."[116] In general, the "software development process for public blockchains is also said to be decentralized, as is typical of open-source software projects."[117] Both "volunteer and paid software developers write and update the software," and as "the code is publicly available," a change can be proposed by anyone.[118] There are more "senior blockchain developers," including, for example, "Bitcoin Core or Ethereum Core developers" who "steer the network's evolution."[119] These core developers can "suggest options regarding the functionality and underlying principles of the network that miners subsequently vote on."[120] Many provide a "service," which is open-source, for no remuneration. Individuals can build upon and alter this.[121] The governance structure in a blockchain system is thus complicated. There are these identifiable groups, and possibly these software developers could be seen as the group really having a significant impact on the structure of the blockchain system. However, this is a peer-to-peer structure

---

114 MICHÈLE FINCK, BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE 51 (2019).
115 Schoers, *supra* note 110.
116 FINCK, *supra* note 114, at 52.
117 Walch, *supra* note 107, at 60.
118 *Id.*
119 FINCK, *supra* note 114, at 52.
120 *Id.*
121 Interview with Thomas Nägele, Managing Partner & Att'y at Law, Nägele Attorneys at Law LLC (Dec. 6, 2019).

where, ultimately, even if there are a variety of core developers, the code is open-source. Modifications can be accepted from different persons who can be situated anywhere in the world. Even if one would consider that it is the core developers that are accepting these decisions, these can still make up a bigger group of persons. One could possibly say that they should be held liable for problems on a blockchain system, yet this would be premised on the idea that they are the central authorities within the system. This would go against the supposedly decentralized nature of blockchain, thereby placing responsibility with a few key individuals.

C. Sub-Meta-level (A): Smart Contracts and Legal Smart Contracts

1. Liechtenstein Contract Law

It is relevant to first consider the basis provided by the Liechtenstein Civil Code on traditional legal contracts in order to compare these with smart contracts. Section 861 of the Civil Code outlines the way in which a contract is formed. An individual makes a promise by allowing their right to be transferred to another, which authorizes the transferee to permit something, give something, or refrain from doing something on the individual's behalf. The crucial point is that if the other individual validly accepts this promise, a contract is formed based on the concurrent expression of intention, referred to as "übereinstimmende Willenserklärung."[122] A contract may also not violate a law or be contrary to public morals (§ 879 FL-ABGB). Furthermore, a contract can be made orally or in written form, in or out of court, and with or without a witness present (§ 883 FL-ABGB).

Once parties have agreed on the contents of a contract, the principle of *pacta sunt servanda* applies. This principle states that both parties have to respect the terms of the contract entered into, as they created a source of law that binds the parties ("lex contractus").[123] If one of the parties does not respect the terms of the contract, the other party is entitled to seek recourse judicially, whereby compliance with the contract is demanded. There are two exceptions to the principle binding the two parties to the agreement. The first exception is if there is a "Leistungsstörung," which could be referred to as a "fault to perform" or "fault in performance." This fault occurs after the conclusion of the contract, where an obligation is not properly performed, or not performed at all. The second exception is if there is a "Wurzelmangel," which occurs when a mistake exists at the moment a contract is concluded. There exists a "defect" or

---

[122] KODEK ET AL., *supra* note 64, at 45. *See also* Interview with Thomas Feldkircher, Partner & Att'y at Law, Nägele Attorneys at Law LLC (Aug. 13, 2019).

[123] KODEK ET AL., *supra* note 64, at 69.

"fault" at the "root," and this error represents a problem in light of the effectiveness of the contract.[124]

2. Smart Contracts

A smart contract is characterized as essentially being a computer program or a program code. Through its source code, a smart contract sets certain conditions which must be met for an action or an event to take place. An automated process thus takes place based on conditions set, which are stored immutably on a blockchain system.[125] An example of smart contract application is the payment of apartment rent, wherein A is the landlord and B the tenant. The smart contract could be encoded so that the action of A opening the door would automatically lead to B receiving the rent payment, which is on a wallet. Opening the door is thus the condition. The smart contract allows this process to be enforced automatically. For, "by turning the key, it is an information which goes…to the code."[126]

Smart contracts exemplify both similarities and differences to traditional legal contracts. There are two striking similarities. First, parties negotiate the terms of the agreement as they would do traditionally. Second, "parties memorialize all or part of their understanding in smart contract code, which is triggered by digitally-signed blockchain-based transactions."[127] Smart contracts differ from legal contracts in that there is no traditional, trusted middleman required. Instead, the smart contract code "is executed in a distributed manner by all the nodes supporting the underlying blockchain-based network."[128] Since smart contracts are "autonomous in nature," obligations memorialized in code are "harder to terminate than those memorialized in a natural-language legal agreement."[129] With no single party controlling the blockchain, challenges arise if a party would want to halt the execution of a smart contract after it is triggered.[130]

As traditional contracts "define rights and obligations for each contracting party that are memorialized via context-sensitive legal prose," the complexity of the rights and obligations affects their translatability into code and affects what function the smart contract will play. Rights and obligations

---

124 *Id.* at 70-71.

125 Sascha Smets, *Smart Contracts im Zivil- und Gesellschaftsrecht*, *in* BLOCKCHAIN RULES 107 (Christian Piska & Oliver Völkel eds., 2019).

126 Interview with Ralph Wanger, Partner & Att'y at Law, Batliner Wanger Batliner Attorneys at Law Ltd. (Oct. 9, 2019).

127 PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 74 (2018).

128 *Id.* at 74.

129 *Id.* at 74-75.

130 *Id.*

that relate to the "exchange of value or the transfer of title to a digitally represented asset" represent promises which are "binary in nature and thus naturally translatable into code."[131] However, a traditional contract may be "open-ended or ambiguous," with parties promising they will act in "good faith" or use "best efforts."[132] At the moment, smart contracts are not able to take into account the "open-ended rights and obligations, which are neither binary nor highly formulaic."[133] This is because the terms are "unstructured" and "hard to predict and thus not suitable for being memorialized into the strict logic of code."[134]

Consider the act of selling a watch. The offer is represented by Party A placing the watch at a certain price. Party B can then accept this offer and transfer money to Party A. An escrow agent may state that the watch was distributed, which would trigger the smart contract to perform the transaction and transfer the money. The escrow agent checking the watch could be the condition set in the smart contract. This condition would in essence also be the condition upon which the two parties agree to the transaction. While this process is set in code, it is performed on the basis that the two parties have a concurring will. This will is itself based on the fact that one party really has the money to transfer and the other party really has the watch. In this example, the smart contract would have a technological function: "the smart contract here would be the transfer agent of your fiat."[135] This returns to the idea that the smart contract is a technical implementing instrument, executing an agreement or a legal contract.

Another example is a smart contract that allows dividends to be distributed directly to shareholders. In this case, the smart contract functions as an "enforcement of ownership, or of a contract with the company, but it is not a contract."[136] This example focalizes on the enforcing role of smart contracts, in which there is no necessity for the usage of "legal means to enforce it," for "it enforces itself."[137] Even the example of the rent payment from A to B, which was conditioned upon the opening of the door to the apartment by A, represented an enforcement. These examples epitomize that smart contracts can "automate payment obligations and the transfer of valuable assets," yet smart contracts cannot "obviate the need for parties to agree to these arrangements."[138] Parties must first negotiate and agree upon terms that are then

---

131 *Id.* at 77.
132 *Id.*
133 *Id.*
134 *Id.*
135 Interview with Thomas Feldkircher, *supra* note 122.
136 Interview with Ralph Wanger, *supra* note 126.
137 *Id.*
138 DE FILIPPI & WRIGHT, *supra* note 127, at 78.

translated into code. In order for the "contractual relationship to emerge via a smart contract, parties still need to manifest consent to stipulated terms by using a digital signature."[139]

In essence, smart contracts can be seen in two ways: as the content of a contract or as the instrument for the conclusion of a contract. The latter view rests upon the idea that smart contracts are programs that function on the blockchain as implementing instruments to execute legal contracts.[140]

3. Legal Smart Contracts

From a legal perspective, a smart contract would not be considered a contract in a strict sense. Even though smart contracts are not considered contracts *sui generis*, they still play a role in the contractual law domain.[141] In this realm, a "legal smart contract" can emerge, which would result in an on-chain conclusion of a contract entirely based on program code.[142] The "Willenserklärung," or expression of intent, has to meet specific criteria to be considered a binding offer within Liechtenstein civil law. The requirements are i) it must be precise as to content and should be legally defined "inhaltlich bestimmt sein" , ii) the essential content which is required by law would have to be included (*essentialia negotii*), iii) the offeror's final intention to be bound should be expressed, and iv) it should be received by the potential contracting party "es sollte dem potentiellen Vertragspartner zugehen" .[143]

Thus, one could speak of a "legal smart contract" in Liechtenstein in certain situations if one considers a concurrent expression of intention by two parties expressed or memorialized by the smart contract, which is translated into code. The language may be different, but this concurrent will provides the basis for the contract.

In general, the status of smart contracts is best summarized as follows: A smart contract is probably both "a contract, and an enforcement, but it is more an enforcement than a contract."[144] It is necessary to "take a close look" at what exactly is being considered, for smart contracts can add further layers.[145]

---

139 *Id.*

140 Smets, *supra* note 125, at 107.

141 Manuel Mofidian, *Smart Contracts im Zivil- und Gesellschaftsrecht*, *in* BLOCKCHAIN RULES 110 (Christian Piska & Oliver Völkel eds., 2019).

142 *Id.* at 115.

143 *Id.*

144 Interview with Ralph Wanger, *supra* note 126.

145 Interview with Thomas Feldkircher, *supra* note 122.

4. Smart Contracts and Civil Law Solutions

The following considers the "fault in performance," or "Leistungsstörung," of a smart contract. The "Leistungsstörung" can take on three different forms: the contract may not be performed at all ("default," or "Verzug"), be performed late, or be performed in an unsatisfactory manner.[146] This section will consider the simple case of defaults, which occur when an obligation is not fulfilled at the proper time, the proper place, or in the manner described.[147]

At this point, the distinction between the "legal smart contract," a smart contract, and a traditional legal contract, is relevant again. The smart contract can represent an additional layer to the traditional legal contract; it is not a part of the legal contract, but rather an enforcement of the legal contract, while the "legal smart contract" is concluded on-chain and rests upon the concurrent expression of intent. This has an impact on how it is dealt with and how the civil law basis applies.

If there is a bug in the code of the smart contract leading to the wrong enforcement of the traditional legal contract, for instance, not delivering the correct amount of money even though it was agreed upon between two parties, it is the obligation within the traditional legal contract which is not fulfilled.[148] Thus, one should look to §918 FL-ABGB for legal remedies. One available remedy is to ask for performance and compensation of damages, where the liability would come into play, which is attributed to the defaulting party. If the counterparties know each other, this situation poses no problem.

Liability for the non-performance of an obligation within a contract would arise from fault-based liability, in which the unlawfulness would specifically be the non-fulfillment of the contract. The problem, however, is not posed by the non-performance of this contract. The problems remain the same as before, and a basic civil law remedy can be found, as is demonstrated by the example. It holds true for Liechtenstein that problems relating to smart contracts can be solved with the "normal civil law instruments."[149]

A possible challenge could arise in the absence of a counterparty or the absence of middlemen. The problems are, more than anything, technical rather than legal. While there may have been a breach of contract on a blockchain system and this could be enforced through traditional civil law, the liability cannot be enforced in the absence of a counterparty. The liability gap persists when there is no party to hold accountable if damages arise.

---

146 KODEK ET AL., *supra* note 64, at 150.
147 *Id.* at 160.
148 Mofidian, *supra* note 141, at 123.
149 Interview with Thomas Feldkircher, *supra* note 122.

5. Legal Smart Contracts and Civil Law Solutions

The "Leistungsstörung" scenario was based on a bug in the code, which affected the act of non-fulfilment after the conclusion of the contract. Since the smart contract was only enforcing the traditional contract and did not represent the legal contract between the two parties, it was easier to look to the Civil Code to find a remedy related to the traditional legal contract. The smart contract, in that case, merely added an automated enforcement layer to the traditional contract. A different approach could be considered with respect to a "legal smart contract," concerning the situation in which there is a problem in the smart contract's coding.

A fault within the legal smart contract, which is present in the forming of the contract ("im Entstehungsakt") is conceptualized differently in comparison to a fault arising after the conclusion of a contract ("im Erfüllungsstadium"), the latter exemplified by the previous example with the "Leistungsstörung."[150] If there is a bug in the legal smart contract itself, this would no longer be considered a fault in performance. The contract would have been concluded with this inherent fault, meaning it would be a "Wurzelmangel," as it is a "defect" or "fault" occurring at the primary stages, or at the "root."[151] Depending on the specific type of "Wurzelmangel" there would be different legal remedies. Since liability is considered, it is important at this point to note that this would give rise to the same liability gap as in the previous scenario. There would be the technical problem that there may not be a counterparty to hold liable. However, if one knows the counterparty with which one is contracting, the traditional civil law basis provides legal remedies.[152]

6. The Other Party in a Legal Smart Contract

The first example illustrated that a "bug" in the smart contract code had an effect on the enforcement of the traditional legal contract. In the second example, there was a "fault," and the concurrent expression of intention was not respected. This resulted in the legal remedy of the "Irrtumsanfechtung," or contestation of error. If the counterparties to a contract understood the coding of a contract, depending on the circumstances, they should have noticed the error in the code or the ramifications that this had (applying § 871 AT-ABGB/FL-ABGB). In that case, the responsibility is in a sense placed on the parties to the contract, rather than the smart contract code developer. However, there may be situations where this does not apply. The parties to a smart contract

---

150 Mofidian, *supra* note 141, at 124.

151 *Id.*

152 *Id.* at 124-125.

may not have the necessary skills to encode a smart contract, or an error may be so minor that a counterparty would not be expected to notice it. Thus, they would have to "hire a third party to create the smart contract," or depend on a "smart contract template offered by a third party."[153] However, there is no established accountability for a mistake in the coding itself due to faults by the developer.

i. The Smart Contract Platform Provider

One should focus on the liabilities arising out of the traditional legal contract when considering the smart contract as an additional layer to the traditional legal contract. However, with legal smart contracts, other contractual relationships also become relevant. One must not only take into account the relationship between the smart contract users (the two parties to the contract), but also the relationship between the users and the smart contract platform providers.

This consideration is analogous to existing situations nowadays. When a buyer makes an order online, a sales contract is not only formed between the buyer and seller, but also a third party (like Amazon) depending on where the order is taking place. In the same fashion, behind different smart contract platforms, there are different organizations which are responsible for the programming, further development, and maintenance of the smart contract platform.[154] A well-known example is Ethereum, a smart contract platform with "a market cap in the billions of dollars,"[155] and backed by the Ethereum Foundation. The Ethereum Foundation published general terms and conditions on its website that are applicable to the use of services and the contents offered on the website. From these terms and conditions, Ethereum's will to conclude a legal transaction can be implied ("Rechtsgeschäft abschliessen").[156]

Once another contracting party has been identified (often the smart contract provider), a party would then have to consider the type of contract it is entering into with the other party. As is the case with established online platforms, the type of contract that is established will vary depending on case-specific circumstances. If one draws a parallel between cloud-computing services (like Google Drive) and smart contract platform providing services, the use and provision of smart contracts could be categorized and classified in a similar fashion. Cloud-computing contracts are divided into either work and service contracts, or rental, custodial, and loan agreements; these contract types

---

153 Stuart Levi et al., *Legal issues surrounding the use of smart contracts*, *in* BLOCKCHAIN AND CRYPTOCURRENCY REGULATION (2020) 162 (Josias Dewey ed., 2018).

154 Smets, *supra* note 125, at 128.

155 Gupta, *supra* note 17, at 28.

156 Smets, *supra* note 125, at 128.

could be applied analogously to smart contract platform providers, depending on how the contract is characterized. Legal remedies and obligations would then arise depending on how one would qualify the specific service.[157] It is not within the purpose of this paper to explore this further. It only remains necessary to say that depending on the contract, there are different legal remedies available.

a. The Smart Contract Platform Provider and the Internet Intermediary

The smart contract platform provider can be compared to the Internet intermediary regulated under the EU E-Commerce Directive.[158] An OECD report suggested a definition for Internet intermediaries, noting that they "bring together or facilitate transactions between third parties on the Internet," specifically giving "access to host, transmit, and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."[159] In a similar fashion, smart contract providers "bring together or facilitate transactions between third parties" on a blockchain system over the Internet. Under the EU E-Commerce Directive, there can be different kinds of internet intermediaries, some of which are internet access and service providers that "offer wired and wireless access to the Internet," and e-commerce intermediaries (such as Amazon) who enable online buying and selling.[160]

In this realm, sanctions can be imposed against the intermediaries. These can naturally arise if "unlawful activities" are "initiated and accomplished by the same intermediaries (violating privacy/data protection, abusing of dominant market power)."[161] Intermediaries could also be subject to "secondary liabilities," which are "triggered by illegal activities initiated by their users,"[162] because the intermediary provides the infrastructure which "enables and facilitates the user's illegal behavior, or magnifies its impacts."[163] However, as outlined in Section 5.5 on the Liechtenstein E-Commerce Law (implementing the E-Commerce Directive), there are exceptions to this liability. For example, providers are not liable if they do not have knowledge of a user's illegal activity, or if they take immediate actions once they do.

---

157 *Id.* at 128-29

158 Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).

159 Giovanni Sartor, *Providers Liability: From the eCommerce Directive to the future*, POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY 4 (2017), https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf.

160 *Id.* at 4-5; *see also* Schoers, *supra* note 110.

161 Sartor, *supra* note 159, at 8.

162 *Id.* at 8-9.

163 *Id.* at 9.

It is helpful to take this framework into account for smart contract providers. The E-Commerce Directive focuses specifically on illegal activities which occur through the infrastructure provided by the intermediary. Such a situation could also arise in relation to a smart contract that facilitates an illegal transaction. Looking at the contractual side, it is questionable whether the contract would even come into being if the essence of the contract is based on an activity that violates a law (§ 879 FL-ABGB), or if it would be "unlawful" if the contract were in violation of a protective law. Considering this more generally, the regulation of the Internet intermediary is in a sense a regulation of the "provider." Applying this idea to the smart contract provider, this can then be compared to the regulation of the "developer." Commissioner Brian D. Quintenz of the Commodity Futures Trading Commission (CFTC) of the United States considered the applicability of accountability in relation to smart contract applications on blockchain networks. Quintenz emphasizes the role of "knowledge or intent," when positing which actors could be held accountable.[164] It is considered "unreasonable" to hold core developer groups accountable without further "evidence of knowledge or intent," as these actors may have no knowledge of the way in which a smart contract has been deployed.[165] The attribution of accountability to miners or users is also considered unreasonable, as these actors "are not in a position to know and assess the legality of each particular application on the blockchain."[166] When considering the smart contract code developers, Quintenz does not condemn the action of developing the code itself, but rather highlights the importance of whether "these code developers could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CTFC regulations."[167] The Commissioner considers different aspects whereby smart contracts could be designed to "resemble traditional financial products," or more generally designed to predict future events, causing a specific contract to fall within the category of prediction markets "where individuals use so-called 'event contracts,' binary options, or other derivative contracts to bet on the occurrence or outcome of future events."[168] Quintenz specifically considers the example of prediction markets, whereby certain contracts could likely qualify as event contracts that depend on the occurrence of a certain event. Event contracts raise public policy concerns and therefore have "a unique spot in CFTC jurisprudence," causing the CFTC to only

---

[164] Brian D. Quintenz, Commissioner, CFTC, Remarks at the 38th Annual GITEX Technology Week Conference (Oct. 16, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16#_ftn9.

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] *Id.*

authorize "off-exchange trading in event contracts in limited circumstances, on specific types of events, for academic purposes, and with strict limits on the amounts retail customers can invest."[169] In this specific example, the development and deployment of event contracts could fall within the regulatory realms of the CFTC. If the code was "specifically designed to enable the precise type of activity regulated by the CFTC, and no effort was made to preclude its availability to U.S. persons," the Commissioner suggests that "a strong case could be made that the code developers aided and abetted violations of CFTC regulations."[170] While this would be at the level of aiding and abetting, the Commissioner indicates that developers who develop code with the intent to violate CFTC regulations could, in this manner, be held liable. This is similar to the provisions in the E-Commerce Directive, as liability is attributed in relation to whether there was "actual knowledge or awareness of illegal activity."[171] In the blockchain ecosystem, if one looks to current regulation, emphasis could thus be placed on "intent" and "knowledge" when assigning liability to different actors. This could be reasonably assumed to extend to other securities regulations, such as those propagated by the Securities and Exchange Commission (SEC). The SEC found that EtherDelta, an online platform that allowed the trading of digital assets, was in violation of Section 5 of the Securities Exchange Act of 1934 because EtherDelta "did not register as a national securities exchange or operate pursuant to an exemption from such registration."[172] Underlying this action was the fact that "operations are defined and executed by EtherDelta's 'smart contract' that runs on the Ethereum Blockchain."[173] In this example, the "provider" was in violation because the platform itself had not been registered. For individual liability of the provider, the SEC's focus was not as much on the role of EtherDelta's founder in writing the smart contract itself, but rather his role as provider and operator of the EtherDelta platform generally. The provider enabled regulated transactions to take place within an unregulated system. This example shows how the E-Commerce Directive could provide guidance, insofar as liability could extend to the founder of EtherDelta, if the founder wrote and deployed the smart contracts with the knowledge that transactions would take place within this unregulated system (if he had "actual knowledge of illegal activity" and was "aware of facts or circumstances from which the illegal activity or information is apparent"). Thus, developer liability could be actively applied with regards to criminal activity. However, this should not be taken to infer that a developer

---

169 *Id.*

170 *Id.*

171 Council Directive 2000/31/EC, 2000 O.J. (L 178) 1 (EC).

172 Zachary Coburn, Admin. Proceeding File No. 3-18888, Release No. 84553 (Nov. 8, 2008), https://www.sec.gov/litigation/admin/2018/34-84553.pdf.

173 *Id.*

of code that is later used by unrelated parties in violation of laws or regulations could be held liable *per se*. "[G]iven the open-source nature of many blockchain projects, developers will have little insight into how their smart contract code is being used, or by whom,"[174] therefore it may be unreasonable to hold a developer liable for actions by unrelated third parties utilizing the developer's code. This is a notion which the E-Commerce Directive also recognized for activities occurring on platforms of Internet intermediaries.

ii. Liability Gaps

With regards to smart contracts, the assignment of smart contract liability is based on the relationship that is being considered.

If there is an error in the code of the smart contract that is enforcing a traditional contract, leading to a "Leistungsstörung," one must determine who is liable for the non-performance, or unsatisfactory performance. The non-performance of the contract arising out of an error in the code does not, in principle, have an effect on the responsibilities that the parties to the traditional contract have. The contractual obligations remain the same. In that sense, it is clear that the liability is still assigned to the party that has not performed the contract.[175] If the smart contract is coded by one of the parties to the contract, then the party should be liable for a mistake in the code. This could be established as one of the obligations within the traditional contract that the smart contract is enforcing.[176] However, the problem is the non-performance itself, which as mentioned, can be resolved. Also, in the case of a bug, the concurrent expression of wills is expressed in the traditional contract and the bug itself does not represent the concurrent will, meaning the smart contract is not part of the content of the traditional contract.[177] In the end, it is important that the contract is fulfilled as it was foreseen. In this sense, the Civil Code closes this "liability gap" when the parties are known, and when one of the parties has coded the smart contract.

It is important to note that one may not know the counterparty when entering into a legal smart contract. When an agreement is entered into by "pseudonymous parties," the parties have "limited ability to affect a smart contract transaction – even if there is a mistake or error in the underlying code."[178] While in this case "enforcement may be difficult, we must not confuse

---

174 Levi et al., *supra* note 1253.

175 Mirjam Eggen, *Smart Contracts und allgemeine Geschäftsbedingungen*, *in* BRÜCKEN BAUEN: FESTRSCHRIFT FÜR THOMAS KOLLER 171 (Susan Emmenegger et al. ed., 2018).

176 *Id.*

177 Mofidian, *supra* note 141, at 123.

178 De Filippi & Wright, *supra* note 127, at 85.

potential for legal liability with the challenge of enforcement."[179] One proposed solution is a type of arbitral tribunal ("Schiedsstelle"). The recourse to this arbitral tribunal could be established by the parties prior to the contract and be pre-programmed into the code. This arbitral tribunal could decide on a programming error, and could, for example, have the ability to reverse a transaction. Since the smart contract can only execute what it is programmed to do, it would be vital that the access to the tribunal, as well as its powers, be pre-programmed.[180]

There are different dimensions to consider if there is a fault in performance ("Leistungsstörung") when the smart contract is coded by a third party. First, the introduction of an external third party can have an effect on the contractual relationship between the two parties of the legal smart contract. It still holds true that the liability is assigned to the non-performing party, which has to either fulfill the contract or provide compensation, depending on the situation. The third party who coded the contract could also be considered an "Erfüllungsgehilfe" (a vicarious agent) of one of the two parties.[181] For, "whoever is obliged to perform a service to someone else is liable to him for the fault of his legal representative as well as of persons who he employs to deliver the performance of the service as for his own" (§ 1313a AT-ABGB).[182] If this form of vicarious liability were to apply, it would be an additional layer where the actions of the third party could possibly be assigned to one of the contracting parties to the legal smart contract.[183] In this case, the Austrian Civil Code would provide the basis for assigning liability.

In addition to affecting the contractual relationship between the parties of the legal smart contract, a mistake in the code may also have an effect on the contractual relationship between the parties to the smart contract and a third party. There is no consensus on the legal nature of an agreement that is based on the transfer of use of a software in return for a fee.[184] For example, for the service contract ("Werkvertrag") and the rental contract ("Mietvertrag"), remuneration ("Entgeltlichkeit") is a precondition, and the "work" or "service" of the third party coding a smart contract could be considered under one of these

---

179 Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 U. ILL. L. REV. 1361, 1396 (2018).

180 Jörn Heckmann & Markus Kaulartz, *Smart Contracts – Anwendungen der Blockchain-Technologie*, 32 COMPUTER UND RECHT 618, 624 (2016).

181 Eggen, *supra* note 176, at 171-172.

182 Erika Pircher-Eschig & Peter Eschig, DAS ÖSTERREICHISCHE ABGB – THE AUSTRIAN CIVIL CODE 313 (Erika Pircher-Eschig & Peter Eschig trans. 2013), *see also* Das Personen- und Gesellschaftsrecht [PGR] [Person and Companies Act], Jan. 20, 1926, § 44 (Ger.).

183 Eggen, *supra* note 176, at 172.

184 *Id.*

contract forms.[185] Whichever contract form one considers, recourse would be possible for the parties to the legal smart contract against the smart contract coder, and liabilities would emanate from the "service" or "rental" contract entered into with the third party.

A smart contract platform provider can provide open-source tools for smart contracts.[186] In this case, a smart contract platform provider is not "hired" by parties entering into a legal smart contract. Consequently, the platform provider then does not "owe" a program or work to parties who enter into a legal smart contract, the basis of which derives from a smart contract platform. Platforms that do not ask for remuneration could then fall under a "Leihvertrag,"[187] or *commodatum*, where no fee is charged for the loan that is made.[188] If it were for remuneration, one could follow the model provided by the Austrian Civil Code, where it could be considered a "freier Dienstvertrag" (§ 1151 AT-ABGB), a type of contract in which the diligent effort to reach an objective represents the contractual obligation.[189]

There is the understanding that "imposing personal liability upon the creator of a public, open-source protocol runs contrary to the common understanding and ethos of the open-source-software community."[190] In the same fashion, a smart contract code developer should not be held liable for the accuracy of the open-source code. But as mentioned, its "open-source nature" places challenges upon developers in foreseeing "how their smart contract code is being used, or by whom."[191]

In each of the examples discussed, the smart contract coder – regardless of whether it was a party to the legal smart contract, a third party hired by one of the parties to the legal smart contract, or a smart contract platform provider – could be seen as entering into a type of contract with another party, and hence could be subsumed under contract law. Thus, the Civil Code would be able to provide the basis for establishing liability. There would also not be a question as to whether a coder *can* be held liable, but rather whether a coder *should* be held liable. However, this is a different discussion outside the purpose of this paper.

---

185 Smets, *supra* note 125, at 130-131.
186 *See, e.g.*, The Accord Project, https://www.accordproject.org (last visited Feb. 16, 2020).
187 Smets, *supra* note 125, at 131.
188 KODEK ET AL., *supra* note 64, at 240.
189 *Id.* at 212.
190 Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. 373, 395 (2019).
191 Levi et al., *supra* note 153, at 162.

D. Sub-Meta-Level (B): Transaction over Blockchain System

1. Token

The following considers the transaction of a token over a blockchain system. It is thus relevant to first define a token.

A token is generally a "representation of something unique."[192] In the context of blockchain, tokens are an "artefact of choice to represent assets, utility, or a claim on something inherent to a specific blockchain project."[193] In general, tokens have no "intrinsic value"; instead, they can "represent assets and be assigned to a specific person or legal entity."[194] From a purely technical point of view, a token is "a set of electronic data."[195]

There are many different types of tokens, which have increased over the years in number and complexity.[196] Their usage is especially frequent in relation to Initial Coin Offerings (ICOs). ICOs involve the transfer of funds by investors, "usually in the form of cryptocurrencies, to an ICO organizer," and in return they "receive a quantity of blockchain-based coins or tokens which are created and stored in a decentralized form either on a blockchain specifically created for the ICO or through a smart contract on a pre-existing blockchain."[197]

Tokens can be used for different purposes and have different functions. They can "represent the right to access a network or a service," "the right[s] pertaining to an object," and "shares in a company or a right to the distribution of a dividend or a bond." They can also "be used for asset transactions in cryptocurrencies."[198] In the context of securities trading for example, in the same fashion as a blockchain "replaces a central bank when administering transfers of digital currency, a blockchain can also serve as a centralized repository for facilitating securities trade."[199] It becomes possible to "tokenize a share of a company, a U.S. treasury Bond, a syndicated loan agreement, or other securities, and rapidly exchange the token like bitcoin."[200] An asset can also be tokenized, which involves the process of turning physical assets into

---

192 Luis Oliveira et al., *To Token or Not to Token: Tools for Understanding Blockchain,* 1 (2018), https://www.zora.uzh.ch/id/eprint/157908/1/To%20Token%20or%20not%20to%20Token_%20Tools%20for%20Understanding%20Blockchain%20Toke.pdf.

193 *Id.*

194 Patrick Bont & Thomas Nägele, *Tokenized Structures and Assets in Liechtenstein Law*, 25 TR. & TR. 633, 633-34 (2019).

195 *Id.* at 634.

196 Oliveira et al., *supra* note 193, at 2.

197 THE FED. COUNCIL OF THE SWISS FED'N SWISS FIN. MARKER SUPERVISOR AUTHORITY, *Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs)* 1 (2018).

198 Bont & Nägele, *supra* note 195, at 634.

199 De Filippi & Wright, *supra* note 127, at 93.

200 *Id.*

digital assets. Through asset tokenization, "real assets" are represented as "digital tokens" that "allow issuers and holders of the tokens to achieve the benefits of cryptocurrency, that is, security, liquidity, and immutability, to real-world assets."[201]

There are different ways to categorize and classify tokens. One method is to distinguish between currencies and tokens. While a currency is "native to a blockchain," the token is "created on top of a blockchain and governed by a smart contract."[202] Many tokens on the Ethereum platform for example are "governed by smart contracts following the common standard called ERC-20, which specifies a set of functions and events that all ERC-20 compliant smart contracts should implement."[203] Using such a differentiation is "based on the technical layer in which the asset is built on, and does not pertain to the role which the asset takes."[204]

The different categorization of tokens has led to the emergence of different "types" of tokens, depending on the attribute considered and definition given. In Switzerland for example, tokens have been split into three groups: asset tokens, utility tokens, and payment tokens. This is based on the guidelines issued by the Swiss Financial Market Supervisory Authority in an attempt to respond to the rise in Initial Coin Offerings (ICOs) and the regulatory issues pertaining to them.[205] ICOs Asset tokens represent "real economic assets" which are "outside the blockchain."[206] Utility tokens are "primarily functional or consumptive in nature, often serving as a means to access and meter an online service," and can "imbue holders with the right to develop or create features for the service, including the right to vote on how the online service should be updated or evolve."[207] Within the Swiss context utility tokens in fact "give access to a digital application or service provided on or via a blockchain-based infrastructure."[208] Payment tokens are tokens that can be accepted by Initial Coin Offering (ICO) organizers as a "means of payment for acquiring goods or

---

201 George Sazandrishvili, *Asset Tokenization in Plain English*, 31 J. CORP. ACCT. & FIN. 68, 68-69 (2020).

202 Yan Chen, *Blockchain Tokens and the Potential Democratization of Entrepreneurship and Innovation*, 61 BUS. HORIZONS 567, 569 (2018).

203 *Id.*

204 Oliveira et al., *supra* note 193, at 5.

205 *See* SWISS FIN. MARKET SUPERVISORY AUTHORITY, GUIDELINES FOR ENQUIRIES REGARDING THE REGULATORY FRAMEWORK FOR INITIAL COIN OFFERINGS (ICOS) 1 (2018), https://www.newsd.admin.ch/newsd/ message/attachments/55153.pdf.

206 FED. COUNCIL OF THE SWISS FED'N, LEGAL FRAMEWORK FOR DISTRIBUTED LEDGER TECHNOLOGY AND BLOCKCHAIN IN SWITZERLAND - AN OVERVIEW WITH A FOCUS ON THE FINANCIAL SECTOR, 83 (2018).

207 De Filippi & Wright, *supra* note 127, at 100.

208 FED. COUNCIL OF THE SWISS FED'N, *supra* note 207, at 83.

services or as a means of money or value transfer."[209] The Swiss Federal Council notes that these distinctions are blurred, as "utility and asset tokens can also have the function of means of payment, as hybrid tokens."[210] While this specific example considered these three types of tokens, they can further be distinguished by "class," or "function."[211] One must look specifically at what is being considered in each context, as there is no overarching definition or categorization.

i. Tokens and the Civil Law Basis

Liechtenstein law does not define tokens. Furthermore, since tokens are sets of data, they do not "qualify as an object in the legal sense."[212] However, Austrian civil law allows for immaterial objects to fall within the legal term "object."[213] This would thus place tokens within the category of objects in the legal sense. Furthermore, interpreted on the basis of Swiss property law, Liechtenstein property law "only allows the acquisition of property regarding physical objects: rights, assets, energy, and aggregates of things or objects that are not considered to be objects in the legal sense."[214] These different considerations represent a challenge in categorizing tokens within the Civil Code.

The legal classification of tokens is a separate issue from the fact that tokens can represent certain rights in the legal system. Tokens "can be shaped in a way that they can represent any right, or, respectively, claim to something, e.g., cash money, property rights, Intellectual Property rights," amongst others.[215] This consideration exemplifies that tokens can bestow different underlying rights upon individuals, which could be underlying voting rights, or underlying rights to an asset. Since tokens can be used in different ways, it is necessary for there to be a legal framework in which the rights can be enforced.

2. Liability Gaps

When considering the transaction of a token, there can be no guarantee that the transaction of the token will result in the transaction of the underlying asset or right. For example, when one considers the transfer of a tokenized diamond, different problems arise; one may not know the counterparty, or if one does know the counterparty, one may not be sure whether one should

---

209 *Id.* at 84.
210 *Id.*
211 Oliveira et al., *supra* note 193, at 8.
212 Bont & Nägele, *supra* note 195, at 634.
213 *Id.* at note 10.
214 *Id.* at 634.
215 *Id.*

engage in the transaction, as there is no certainty that the underlying asset will be transferred. Furthermore, without knowing the counterparty, there can be no attribution of liability. However, this problem is inherent to engaging in transactions with pseudonymous parties. If one engages in a transaction with a counterparty one knows, previous considerations would apply as under contract law. On the contractual law basis, a party would have to fulfill its obligations. However, when considering tokens, contract law cannot ensure the transfer of the underlying right. The layer that is added in terms of liability will thus be considered when analyzing the Liechtenstein Blockchain Act.

VII. LIECHTENSTEIN BLOCKCHAIN ACT

A. Introduction

The Principality of Liechtenstein enacted the Token and Trusted Technology (TT) Service Providers Act ("Gesetz über Token und VT-Dienstleister"; "TVTG"), also known as the Blockchain Act, which came into force on January 1, 2020. The purpose of the law is to ensure trust and confidence in digital rights (particularly in the financial and business sectors) to protect users on TT systems, as well as to create optimal innovation and technology-neutral framework conditions for the provision of services on TT systems (Art. 1 TVTG).

The idea of "trustworthy technology" is a central concept within the Blockchain Act. For, in this framework, trust is seen to be "created by technology and not solely by organizations," which "tipped the scales in favor of using the term trustworthy technology as a connecting point in the law."[216] In the Blockchain Act, the term trustworthy is "understood to refer to the integrity of tokens which are clearly allocated to an owner and the secure exchange of which must be ensured."[217] Using the more abstract term "trustworthy technology" instead of "blockchain" was done in order to highlight the trustworthiness inherent to blockchain technology. This link between the two concepts is derived from blockchain's main characteristics of decentralization and immutability, enabled through cryptography, which maintain the integrity of tokens.[218] Furthermore, by adopting "a more definitionally agnostic legal framework," the Blockchain Act could "encompass all aspects of this new and ever growing and changing area of

---

216 GOV'T OF THE PRINCIPALITY OF LIECH., UNOFFICIAL TRANSLATION OF THE GOVERNMENT CONSULTATION REPORT AND THE DRAFT LAW ON TRANSACTION SYSTEMS BASED ON TRUSTWORTHY TECHNOLOGIES, 39 (2018).

217 *Id.*

218 Thomas Nägele & Nicolas Xander, *ICOs and STOs im liechstensreinischen Recht*, BLOCKCHAIN RULES, 390 (2019).

technology."[219] Blockchain has a wide area of application, and is not just linked to cryptocurrencies and token offerings. The Government of Liechtenstein took this into account when drafting the Blockchain Act in order to create a legal basis for the token economy in its entirety. [220]

In summary, the Government of Liechtenstein pursued three specific goals summarized by the Director of the Office for Financial Market Innovation of the Government of Liechtenstein:

> First, to provide legal security for Blockchain companies, their clients and/or Token holders in general. Second, we the government of Liechtenstein want to increase the level of customer protection in relation to the various Blockchain service providers and roles. And third, we want to clarify the rules for AML-compliance. Our law is not focusing on the current applications of the Blockchain Technology, but covering also many future applications of this technology in the digitalization of our economy (so-called Token Economy) by focusing on the underlying mechanisms and roles/service providers.[221]

This re-emphasizes the importance of creating a law broad enough to allow for further development and improvement in the future. At the same time, the Blockchain Act seeks to provide legal certainty for actors within the token economy and sets forth expectations for parties engaging in different types of interactions with one another in this ecosystem.

B. Liability and the Liechtenstein Blockchain Act

1. Liability, Accountability, and Trust

Trust is a "highly ambiguous concept" that has different implications depending on the interaction one is considering. An individual can place their trust in another counterparty, in an institution, or even in a social system as a whole. This consideration exemplifies that there can be different "types" of trust. There can be "personal trust" that allows "individuals to accept vulnerability and place their welfare in the hands of other parties, expecting

---

[219] Alexis Esneault & Thomas Nägele, *Digital Asset Regulation – A cross-country analysis*, 139 (2019).

[220] Nägele & Xander, *supra* note 2180, at 391.

[221] Interview with Clara Billek, Office for Fin. Mkt. Innovation, Gov't of the Principality of Liechtenstein & Thomas Dünser, Dir. of the Office for Fin. Mkt. Innovation, Gov't of the Principality of Liechtenstein (Oct. 2, 2019).

positive intentions and behavior from other parties."[222] Personal trust could, for example, come into play when entering into a contract with another party, and is distinguished from the trust that individuals place in institutions and organizations. "System trust" is related to the confidence placed in "the functioning of systems and that those systems repetitively generate reliable results in a trustworthy way." [223] With respect to organizations, emphasis is placed upon "three organizational trustworthiness factors", which are "ability," "benevolence," and "integrity."[224] Whether one considers the personal, system, or organizational level, trust is focused on the outcome of a situation. Trust relies on the expectation that another person will act with "positive intentions," that the system will be "reliable," and that at the organizational level, there is a sense of altruism and honesty. In essence, these different types of trust are interlinked and serve to support one another. Inherent to the concept of trust is the belief in the righteousness of the other party, who will not default. Trust also involves an acceptance of vulnerability.

In this context, "accountability" plays a key role. Accountability is a principle that ensures "individuals, organizations, and the community are responsible for their actions and may be required to explain them to others."[225] However, accountability "does not just arise, unconsciously or inevitably."[226] Instead, this must be "instilled in a person, or an organization, through a clear identification of rights and obligations."[227] Legal acts can identify these necessary rights and obligations of different parties and, with the right institutions, enforce them. Accountability and trust are inextricably linked: while trust is "the belief in the responsibility of others," accountability "is the tool that ensures that trust is not misplaced."[228] Persons and organizations can be held accountable through responsibilities and obligations they must respect that are enshrined in the law. This then allows citizens to "offer their trust if they feel it will be respected and safeguarded."[229]

A natural person or legal entity can be held accountable for actions or events, as liability bestows legal obligations upon parties.[230] Legal institutions can hold parties accountable because they allow liability to be enforced and

---

222 Dorothea Greiling, *Accountability and Trust*, *in* THE OXFORD HANDBOOK OF PUBLIC ACCOUNTABILITY 2 (Goodin E. Robert ed., Oxford 2014).
223 *Id.* at 3.
224 *Id.*
225 Laura Millar, *An Obligation of Trust: Speculations on Accountability and Description*, 69 THE AM. ARCHIVIST 60, 60 (2006).
226 *Id.* at 61.
227 *Id.*
228 *Id.*
229 *Id.*
230 Ivo Giesen & François G.H. Kristen, *Liability, Responsibility and Accountability: Crossing the Borders*, 10 UTRECHT L. REV. 1, 2 (2014).

maintain the trust in the system. In the sense of the Blockchain Act, the fact that a party is liable for their actions justifies the trust. It is postulated that "it is all about liability, because all other things…derive from liability."[231] The potential of the token economy rests upon the conception that one can "reproduce the 'real world' digitally in a legally certain manner and transmit rights efficiently."[232] Trust itself is a key factor in the token economy, for buyers need "confidence that he/she will actually receive the digital rights to a product or an asset," confidence that the rights can be enforced "in accordance with the rule of law," and "confidence in the companies and individuals who provide services on TT systems."[233] Trust is linked closely to the "confidence" in the legal system and the knowledge that a party will be liable for their actions.

The interplay between trust and liability can most notably be understood when distinguishing between a centralized and a decentralized system. In a centralized system, it is trust that follows liability. However, "in a decentralized system, the liability follows the trust, but it is your liability to play by the rules."[234] In a centralized system, one trusts a central counterparty such as a bank, because they are liable "to the regulator when it comes to supervisory law" under civil law.[235] However, in a decentralized system, trust should be inherent to the system. There is no interest in engaging in a trustless system. In turn, if a transaction is to occur over a blockchain system, there is no incentive for the persons hosting a decentralized ledger to falsely represent the transaction, unless they are possibly bribed. The likelihood of a false representation of a transaction can also be minimized when more hosts are involved in a decentralized system, as there are "less chances . . . for convincing the majority."[236] On a decentralized system with millions of hosts, it is a lot harder to convince a majority of these individuals that a transaction did not occur, or to bribe such a great subset of individuals.

As noted above, distinguishing between centralization and decentralization can depend upon whether trust follows liability or liability follows trust. The considerations exemplify that regardless of whether trust derives from liability or vice versa, both are necessary within centralized and decentralized systems. It is important to note that decentralization does not remove the role of regulation. In the decentralized world, legal liability would follow the trust; for "institutional trust is still needed," as one "still needs people

---

231 Interview with Thomas Feldkircher, *supra* note 122.
232 GOV'T OF THE PRINCIPALITY OF LIECH., *supra* note 217, at 44.
233 *Id.*
234 Interview with Thomas Feldkircher, *supra* note 122.
235 *Id.*
236 *Id.*

to be responsible for these systems."[237] The focus should thus not be on "a question of either/or centralization or decentralization " but rather on enabling "these technological advances by bridging them and integrating them in the existing system by defining the thresholds and requirements for the actors, chang ing the system where necessary and protecting the single citizen and member of a society."[238] The "concept of decentralization is multilayered,"[239] and while one "can use the technology without having the need for a central authority," one can try to find other solutions which allow for an optimal outcome.[240] It is necessary to have a legal system to fall back upon, especially once problems appear. This also touches upon an "ethical aspect": when considering "AI supported or based blockchains" that "govern themselves," it is unclear "what kind of higher institution or higher morals or ethics" one should refer to.[241] If then there is no "higher institution that orients that, it can go wrong," especially if one does "not know what to orient this development on, or if there are conflicting interests."[242] With the Blockchain Act, centralization is not enforced, but instead, the Blockchain Act stipulates "that there are stakeholders, within a decentralized token, or economics, or ecosystem, which guarantee that our trust in decentralisation is justified."[243] The Blockchain Act thus brings together notions of trust and liability, allowing the legal regime to strengthen the trust inherent within the decentralized system.

Figure 2 indicates that interviewees perceive Liechtenstein as performing well in the international arena in terms of introducing liability for business in the blockchain. Of the survey respondents, the majority stated that Liechteinstein is performing at a "very satisfactory" or near very satisfactory rating The next section will shed light upon whether this is really the case. Additionally, it will explain whether, the Blockchain Act has responded to the identified liability gaps and how it goes about doing so.

C. Response to Liability Gaps

1. First Meta-level: Blockchain System

The Liechtenstein Blockchain Act regulates different actors within a Token Economy instead of simply focusing on the underlying technology. The

---

237 Esther Shein, *How Blockchain Changes the Nature of Trust*, THE LINUX FOUND. (2019), https://www.linuxfoundation.org/blog/2019/01/how-blockchain-changes-the-nature-of-trust/.

238 Interview with Clara Billek & Thomas Dünser, *supra* note 222.

239 *Id.*

240 Interview with Thomas Nägele, *supra* note 121.

241 Interview with Clara Billek & Thomas Dünser, *supra* note 239.

242 *Id.*

243 Interview with Thomas Feldkircher, *supra* note 122.

Blockchain Act introduces regulated middlemen, such as the physical validator (who is discussed in section 7.3.3), and the TT Token Depositary. The scope of the Liechtenstein Due Diligence Act ("Sorgfaltspflichtgesetz"; SPG) extends to these actors, as they must abide to due diligence requirements.[244] In fact, the Due Diligence Act was amended to include "TT Service Providers" (Art. 3 para. 1 lit. r SPG). Due diligence duties generally include the identification of contractual partners, "or, in case of the respective partner being a legal entity, its ultimate beneficial owners (Know Your Customer (KYC)/ Anti-money laundering (AML) process)."[245] As a result, the standard that must be respected in the token economy is raised, lowering the liability risks. Furthermore, having actors such as the Physical Validator allows liability to be attached to a party and closes previous liability gaps. Thus, by assigning liability to different actors throughout the system, and ensuring best practices, the blockchain system better balances legal liability.

2. Sub-Meta-level (A): Smart Contracts and Legal Smart Contracts

The liability gap is represented by the fact that in certain situations, one may enter into an agreement with a party wherein they cannot identify their counterparty. While there would be a party to hold accountable, there would be no way to enforce an agreement, as this counterparty would be anonymous. However, this issue has been recognized as a technical problem, rather than a legal problem. The Blockchain Act does not provide a solution to this, as this is a problem of technical nature.

The Blockchain Act indirectly affects the liability risks related to smart contracts. For example, TT Service Providers are regulated and must adhere to certain requirements, such as being reliable in terms of the law. A TT Service Provider could be encoding a simple smart contract, and in this sense, the Blockchain Act indirectly applies a standard of good practices upon smart contracts encoded within this framework. This somewhat reduces the liability risk, as the parties are held to certain standards.

---

244 Bont & Nägele, *supra* note 195, at 637.
245 *Id.*

3. Sub-Meta-Level (B): Transaction over Blockchain System

i. Token Container Model

The Token Container Model (TCM) "lies at the heart of the TVTG."[246] In this model, a token is conceptualized as a container, which has the "ability to hold rights of all kinds, whether that be the right to something represented – examples include real estate, stocks, bonds, and gold; or nothing – encompassing digital code, the most notable example being Bitcoin."[247] There should be no restrictions upon the types of rights that can be represented within the container. Therefore, an "empty" container can exist wherein there is no represented right (as shown with Bitcoins,[248] which "are not backed by real assets").[249] By representing any type of rights, the TCM allows for legal certainty both for "pre-existing rights that are tokenized, as well as rights to digital information on blockchain-based systems."[250]

ii. Token Ownership

The Blockchain Act regulates the right to "dispose of and transfer the token."[251] A distinction is drawn between the "person entitled to dispose of a token" ("owner of a physical object"; "Verfügungsberechtigt"), and the "person factually holding the power of disposition" (possessor; "Verfügungsmacht").[252] In order to express the person entitled to dispose of a token and the person with the actual power of disposition legally, the Blockchain Act introduced the TT-Key ("VT-Schlüssel") and the TT-Identifier ("VT-Identifikator"). The TT-Key (which would be similar to the "private key") allows for the disposal of a token, while the TT-Identifier (which would be similar to the idea of the public key) allows for the clear assignment of the tokens. The TT-Identifier is "generally assigned to a person," which could be "the person entitled to dispose of the token or also service providers."[253] The Tokens are "assigned to an address, known as the 'TT Identifier'," and "can be disposed of via the TT-Key."[254] With the TT-Key, an individual would be entitled to dispose of a token; this may not

---

246 Nägele Attorneys at Law LLC, *Executive Summary* of the "Tokens and TT Service Providers Law" AKA the "Liechtenstein Blockchain Act", at 2 (2019) https://www.naegele.law/downloads/TTTL_Summary.pdf.

247 *Id.*

248 Nägele & Xander, *supra* note 2180, at 394.

249 Bont & Nägele, *supra* note 195, at 636.

250 Nägele Attorneys at Law LLC, *supra* note 247, at 2.

251 GOV'T OF THE PRINCIPALITY OF LIECH., *supra* note 217, at 54.

252 Bont & Nägele, *supra* note 195, at 636.

253 *See* GOV'T OF THE PRINCIPALITY OF LIECH., *supra* note 217, at 61.

254 *Id.* at 70.

be equivalent with the right of disposal.[255] It is assumed that the individual that holds "the private key of a token is also entitled to validly dispose of the token."[256] Thus, in the event that a "third party gains *de facto* power of disposal over the token and can therefore initiate transactions," the third party would not be entitled to dispose of it.[257] Furthermore, the person entitled to dispose could delegate the right of disposal to a TT Service Provider like the TT-Key Depositary, giving the TT-Key Depositary the *de facto* power of disposal.

The right of disposal to the token is similar to the "right of ownership to a physical item."[258] Building upon property law, the transfer of a token under the Blockchain Act requires "a contractual transaction (Verpflichtungsgeschäft)," "the material transfer (Verfügungsgeschäft)," and "an *in rem* agreement on the transfer of the ownership."[259] The Blockchain Act also foresees and regulates the "acquisition of property in good faith by means of transfer of a token from someone not legally entitled to dispose of it."[260] It may be that a holder of a private key is not entitled to dispose of a token.[261] In such a case, the abstraction principle is followed due to the immutable nature of transactions on a TT System.[262] It follows that when disposing of tokens, they are considered valid, "even if a valid obligation-creating contract has not come about (e.g. on account of unlawfulness) or has been subsequently rescinded."[263] In this case, the disposition can be reversed in accordance with the law of enrichment.[264] Furthermore, as in property law, where one can find records of an acquisition of property in good faith, one can look to the "Registriereintrag," or registry for a record of transfers within a blockchain system.[265] This is because the blockchain is in itself a registry that allows one to find the information on the transfer of the token, which can also "facilitate proving that the private key was lost or stolen."[266]

---

255 *See id.* at 9.

256 Bont & Nägele, *supra* note 195, at 636.

257 *See* GOV'T OF THE PRINCIPALITY OF LIECH., *supra* note 217, at 62.

258 REPORT & APPLICATION OF THE GOVERNMENT TO THE PARLIAMENT OF THE PRINCIPALITY OF LIECH., CONCERNING THE CREATION OF A LAW ON TOKENS AND TT SERVICE PROVIDERS (TOKENS AND TT SERVICE PROVIDER ACT; TVTG) AND THE AMENDMENT OF OTHER LAWS, 54 (2019) at 63.

259 Bont & Nägele, *supra* note 195, at 637.

260 *Id.*

261 REPORT & APPLICATION OF THE GOVERNMENT TO THE PARLIAMENT OF THE PRINCIPALITY OF LIECH., *supra* note 259, at 64.

262 Nägele & Xander, *supra* note 2180, at 395.

263 REPORT & APPLICATION OF THE GOVERNMENT TO THE PARLIAMENT OF THE PRINCIPALITY OF LIECH., *supra* note 259, at 64.

264 Nägele & Xander, *supra* note 2180, at 395.

265 *Id.* at 395-396.

266 Bont & Nägele, *supra* note 195, at 637.

iii. Physical Validator

The Blockchain Act builds upon pre-existing law and ensures "that the underlying right represented by the token is effectively transferred from party A to party B."[267] Civil law provides the basis for "what constitutes an effective transfer of property."[268] The Blockchain Act further develops this civil law basis in terms of an effective transfer of *tokenized* property, stipulating that the "transfer of a token on a TT system constitutes a binding transfer of the underlying right, whether that be a right to a physical object or a digital asset."[269] There is emphasis on the underlying right embodied in a token. A token which represents a diamond in that sense does not just represent this object, but rather the underlying right to the diamond.

In order to verify that the underlying right embodied by the token exists, a bridge was created between the online and offline world through the introduction of the function of the "Physical Validator" in the Blockchain Act.[270] The Physical Validator is defined in Art. 2 lit. p TVTG as a person who has to guarantee the enforcement of rights represented by tokens within the meaning of property law on TT-Systems ("eine Person, welche die vertragsgemässe Durchsetzung von in Token repräsentierten Rechten an Sachen im Sinne des Sachenrechtes auf VT-Systemen gewährleistet"). In other words, the Physical Validator's role is to "ensure that the party tokenizing the right to something represented online is in fact the person who possesses that right offline."[271] The Physical Validator must guarantee this,[272] and is liable if rights to the property guaranteed by the Physical Validator are not enforceable in accordance with the contract (Art. 17 lit. e TVTG). This is because when "physical goods are involved, or rights, contained in a token, with respect to a physical good," it is necessary having middlemen that can for example guarantee the existence and owner of the physical good, that the good is not pledged or lost, and that ownership of the good can be transferred to another party.[273] Additionally, this avoids conflicts between the online and offline world. For instance, if one wishes to transfer ownership of a tokenized car, there are two ways: a) one could transfer ownership in the offline world, by *traditio,* from A to B; or b) since the car is tokenized, then the token could be given to a party B, who would then have a right over the car. However, a conflict could arise if the token were transferred to another party, C, while the car itself has

---

267 Nägele Attorneys at Law LLC, supra note 250, at 2.
268 *Id.*
269 *Id.*
270 Interview with Thomas Nägele, *supra* note 121.
271 *Id.*
272 Mauro Casellini et al., *Liechtensteinisches Blockchain-Gesetz*, Blockchain Rules 369 (2019).
273 Interview with Thomas Feldkircher, *supra* note 135.

already been transferred to party B. To prevent a conflict in such a situation, the physical validator was created.[274]

iv. Token Issuance Basic Information

Another actor created through the Blockchain Act is the Token Issuer, which is "a person or entity offering tokens to the public on its own behalf or that of another person or entity"[275] (Art. 2 lit. k TVTG). Each Token Issuer has a duty to provide basic information before a token issuance (Art. 30 TVTG), a concept modelled on the Securities Prospectus Act ("Wertpapierprospektgesetz"; WPPG). Art. 35 TVTG indicates that:

If any facts in the basic information that is to be prepared according to this Act are incorrect or incomplete, or if the basic information in accordance with these provisions was not prepared, the persons responsible under articles 33(3) and (4) shall be liable to every user for damages that arise as a result, provided they do not demonstrate that they took the due care of a prudent businessman when preparing the basic information. Only damage directly suffered is considered to be damage, not also loss of profit.

Token issuers have a duty to ensure that correct information is provided. In cases where they do not, buyers have a legal basis to fall back on. Thus, there is a clear legal liability basis to protect parties with respect to token issuance.

v. Solution in Terms of Liability

With respect to the transaction of a token over a TT-System, through the Token Container Model, there is a conceptual basis upon which the transaction of a token results in the transaction of the underlying right. The Liechtenstein Blockchain Act resolves one possible liability gap by introducing a middleman, the Physical Validator. For example, if there is a transaction of a token representing the right to a diamond from A to B, a physical validator would check that the diamond exists and that A is entitled to dispose of the diamond. This would guarantee that A could transfer the token to B.[276] This "guarantee," in essence, enforces the trust within the transaction. The Consultation Report had even mentioned that the Physical Validator must "ensure that the person possessing the power of token disposal ha d a direct claim against either the Physical Validator's insurance company or the insurance company for the specific property item,"[277] whereby the Physical Validator would have been

---

274 Interview with Ralph Wanger, *supra* note 126.

275 Nägele Attorneys at Law LLC, supra note 247, at 3.

276 *See* Thomas Nägele, Presentation, Token and TT Service Provider Act, Token- und VT-Dienstleister Gesetz (TVTG) (June 29, 2019).

277 GOV'T OF THE PRINCIPALITY OF LIECH., *supra* note 217, at 140.

jointly and severally liable.[278] This exemplifies that the liability question took on a central role in the government's deliberations, especially in terms of the transfer of a token. However, this suggestion was not completely adopted in the final version of the Blockchain Act. Instead, the Blockchain Act limited itself to saying that Physical Validators should have internal control mechanisms in place to ensure "their liability in the event that rights to property guaranteed by the Physical Validator cannot be enforced in accordance with the contract." (Article 17 para. 1 lit. a TVTG).[279] The approach of the Liechtenstein government was to introduce "middlemen in the ecosystem where it is absolutely necessary, to provide the market with some stability and security."[280] In the case of the transfer of a token, without the Physical Validator, there would have been no guarantee or knowledge of whether a token could be disposed of, or whether this token had already been transferred to another party *in corpore*. A level of trust is introduced through the creation of the middleman, who is legally liable, and against whom claims can be enforced. Furthermore, the introduction of the middleman was possible without having centralization in the system. The entire process remains decentralized, yet there is a party which can be held liable. In this scenario, the liability gap was closed through the Blockchain Act.

VIII. Possible Solutions to Remaining Liability Challenges

A. First Meta-Level: Blockchain System

1. Fiduciary Duties

It was outlined that the governance structure of public blockchains is complicated and challenging to understand. One must determine where liability would land in this new constellation with the different actors because a shift of trust has taken place:

> The need to trust in others has simply moved from its traditional place (e.g. the officers and directors of a bona fide corporation), leaving us to discern where it has landed. In these systems that operate money, smart contracts, and potentially many other critical human practices, people continue to lead and make important decisions on behalf of others; we just have to name them and decide how to treat them.[281]

---

[278] Casellini et al., *supra* note 273, at 369.

[279] Report & Application of the Government to the Parliament of the Principality of Liech., *supra* note 259, at 130.

[280] Interview with Thomas Feldkircher, *supra* note 135.

[281] Walch, *supra* note 107, at 59.

There are different possibilities which could be considered to assign liability to a party within the governance structure of the blockchain system. These possibilities become clear when comparing software developers to fiduciaries in public blockchains.[282]

There are certain groups within blockchain systems that make "decisions about the software that operates public blockchains," which can include "people who write software code, make decisions about policies that should be reflected in software code, review software code," and "exclude[ ] miners and other nodes in the network that run the software."[283] There are "core developers," who "generally lead the software development process."[284] An example is provided by Bitcoin, whereby core developers can "send emergency messages to all nodes in the network and are the only developers who have 'commit access' that allows them to make actual changes to the software code."[285] The core developers also exercise power in the public by meeting with international regulators and leaders to express their views.[286] To a certain extent, power is placed with a single group, similar to fiduciaries.[287]

The developers of public blockchains can be compared to fiduciaries, as they exhibit four similar characteristics: i) they provide "socially desirable services" that require sector-specific expertise; ii) they are entrusted with property or power; iii) they have the possibility of misusing their position of power; iv) their actions may make entrustors vulnerable and unable to protect themselves. The first characteristic goes back to the idea that software developers are providing a service. This includes "conducting research, reviewing the code, proposing conceptual changes to the code, reviewing changes proposed by other developers, drafting new code and revising existing code, security-testing new code, compiling code into new releases, and communicating about the project with other developers."[288] These services also require a certain skillset, even if the development of the code is open-source. The services can provide benefits to society; thus, they can be socially desirable. The second characteristic applies to developers, as they are in a position in which they must take significant decisions, especially when considering hard forks.[289] With respect to the third characteristic, developers could take advantage of their position, and directly or indirectly harm other individuals. This could take the shape of developers "failing to discover and fix a security

---

282 *Id.*
283 *Id.* at 58.
284 *Id.* at 61.
285 *Id.*
286 *Id.*
287 *Id.* at 64.
288 *Id.* at 65.
289 *Id.*

flaw in the code, misjudging the risks of a proposed change to the software, or acting in a way that causes regulators to lose faith in the blockchain, all of which could seriously damage those relying on the blockchain."[290] Finally regarding the fourth characteristic, persons without software expertise could still be part of the blockchain ecosystem, for example by engaging in a token transaction. The active involvement of users could place them at serious risk due to the existence of a knowledge barrier between developers and users. The four characteristics outlined are ones shared by all fiduciaries, denoting that certain developers are similar to fiduciaries.

Recognizing these parties as fiduciaries opens more possibilities for assigning liability. This would not be in line with the current attribution of liability in relation to developers: generally, professionals designing or creating software are not subject to claims of professional malpractice, and developers are not liable for harm incurred by third parties from the software created or developed.[291] However, not all developers fall into the category of fiduciary:

In a spectrum of 'fiduciary-ness', those developers who make the most decisions on behalf of others look a lot like fiduciaries, while those who occasionally make code proposals do not. Fiduciary developers would likely include developers who initially design and/or launch the system, those involved in decision making around new releases of software, including policy and technical choices as well as code review, and those who make decisions about how to address a crisis faced by the system (e.g. a critical bug or an attack on the system).[292]

Once certain developers have been identified as fiduciaries, liability can be attached to those developers. They would have to fulfil different duties, whereby the "basic fiduciary duties of care and loyalty are a good starting point."[293] Even if software developers could try to disclaim any potential liability, fiduciary duties can arise through different channels, for example by contract, statute, or status.[294] This would allow entrustors to "have a cause of action against the fiduciaries for a breach."[295] It remains a question, how a programmer could then respond to this liability only from an economic point of view,[296] as "the cost of making whole an entire blockchain would simply be too

---

290 *Id.* at 67.
291 *Id.* at 69.
292 *Id.* at 72.
293 *Id.* at 73.
294 *Id.* at 73-74.
295 *Id.* at 75.
296 Interview with Virginia Cram-Martos, Project Leader of Blockchain Whitepaper Project, United Nations Ctr. for Trade Facilitation and Elec. Bus. (UN/CEFACT),
Co-Leader of Internet of Things in Trade Facilitation Project, CEO, Triangularity SàRL (Nov. 19, 2019).

great."[297] The duties of care could also be adapted and focus on "choosing the right system for the right task and skills," "monitoring the system," and "maintaining the system."[298]

Alternatively, an insurance system, similar to directors' and officer's insurance, could satisfy the many liability claims that could arise.[299] For, "the more frequent or severe potential harm resulting from emerging digital technology, and the less likely the operator is able to indemnify victims individually, the more suitable mandatory liability insurance for such risks may be."[300] In other sectors, "the insurance industry is actively working on developing standardized terminologies and policies for data breaches, hacking, and identity theft," and "are seeking to understand the risks that individuals and companies face and how to price insurance products that would protect people from these developments."[301] However, depending on the magnitude of a problem, an insurance scheme may only help to a limited extent. The insurance system would not work in a catastrophic scenario of the blockchain system where all individuals seek recourse from an insurance provider.

i. Legal Personality and Liability

Liability could also be attached to the system if one takes the traditional legal forms presented by the law when considering the blockchain system. This perspective would recognize the blockchain system in the form of an established structure, wherefrom its legal personality would derive, further allowing the rights and obligations to follow from the legal form the blockchain system takes on.[302]

The system could be considered a business trust, whereby the "protocol" represents the "assets of the business corporation."[303] For the Bitcoin blockchain, the blockchain itself would be the "asset of the business trust," while "the nodes with the power to validate transactions (generally, the miners) are the trustees."[304] The nodes that validate transactions would make decisions related, for example, to hard forks and thus the direction in which the system is

---

297 Walch, *supra* note 107, at 76.

298 *Liability for Artificial Intelligence and other emerging digital* technologies, EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, EUR. COMMISSION 7 (2019), https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.

299 Walch, *supra* note 107, at 76.

300 EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *supra* note 299, at 9.

301 Martin Eling, *How insurance can mitigate AI risks*, BROOKINGS INST. (2019), https://www.brookings.edu/research/how-insurance-can-mitigate-ai-risks/.

302 Walch, *supra* note 107, at 76.

303 Reyes, *supra* note 191, at 411.

304 *Id.*

to go. Some nodes could even be paid for their services. Within this framework, "individuals holding bitcoin act as certificate holders."[305] Holding bitcoin would be equivalent to holding a share in the business trust, and this could be transferred to "others interested in buying into the business trust."[306] The value of bitcoin is determined by "the relative success of the Bitcoin blockchain and the services it provides at any given time."[307] This example indicates that a DLT could be conceptualized as a business trust. While there would be many challenges related to this, this would mean that the DLT protocol could have legal personality:

> In other words, a blockchain may be recognized as a person. Even the mere possibility for this proposition to come to fruition opens unique and important lines of inquiry for issues of corporate governance, DLT protocol governance, and the doctrine of corporate personhood. [308]

This legal separate personhood implies that the DLT protocol would also have limited liability, or be shielded by the corporate veil, which would "protect unsuspecting users and open-source software creators from unexpected unlimited personal liability," while not stifling innovation.[309] Thus, it would not require a developer to hold liability; placing liability on the developer would even "run directly contrary to the economic choice made at the time of the protocol's creation."[310] Yet taking on such a structure could go against the "core ideal of decentralized governance in public blockchain systems."[311]

Under Liechtenstein law, considering the blockchain system from this light would be practically possible, as there are different legal persons under which the system could fall from a corporate law perspective: it could be a "Genossenschaft" cooperative , a "Verein" association , or even a "einfache Gesellschaft" simple corporation as the "prerequisites for building such a simple corporation (einfache Gesellschaft) are not too high".[312] From a "supervisory perspective . . . it could be a fund".[313] A possible solution, in terms of allocating liability to the blockchain system, is to analogously apply one of these corporate structures to this area. The blockchain would be structured in a

---

305 *Id.* at 412.
306 *Id.*
307 *Id.*
308 *Id.* at 413.
309 *Id.* at 395.
310 *Id.* at 395.
311 Walch, *supra* note 107, at 76.
312 Interview with Thomas Feldkircher, *supra* note 235.
313 *Id.*

corporate form, and liability could be attributed accordingly. This could be combined with the idea of the insurance scheme.

ii. Permissioned System

On a permissioned blockchain, liability could be addressed differently, as there is a more identifiable group or counterparty in charge of the blockchain. However, a permissioned system would not be considered a trusted technology in relation to the Blockchain Act, as the rules could be changed by a small number of persons.[314] A permissioned blockchain can be seen as a "software solution,"[315] and while parties can then be identified and one can know upon whom liability would be placed, this would not be a trustworthy system. Thus, this seems to resolve some liability challenges since parties are identifiable. However, since it would only apply to a small subset of the entire system, other issues would arise, such as the fact that the system would be at the whim of a small group of individuals.

However, such challenges have been mitigated by introducing codes of conduct and reliable partners within the system. For example, Cardossier is a "blockchain-based digital dossier in which all relevant information about the entire life cycle of a vehicle can be stored in a traceable and secure manner"[316] and is "implemented on the basis of a permissioned blockchain."[317] Cardossier allows the management of a private-public partnership, in which both private and public actors represent nodes within the ecosystem. Cardossier by-laws (Art. 28-32) represent the foundation which establishes a data protection committee that oversees the enforcement of data protection rights and ensures compliance with the GDPR. The data protection laws and regulations, as well as the compliance and due diligence requirements, make up the code of ecosystem which the members (or nodes) within Cardossier must comply with.[318] In this system, actors are made up of regulatory offices such as the Road Authority of the Principality of Liechtenstein and of the Canton Aargau, financial service institutions such as PostFinance and Multilease, and insurance companies such as AXA.[319] Having a governmental office as part of this system

---

[314] Interview with Thomas Nägele, *supra* note 121.

[315] *Id.* ("A permissioned blockchain can be seen as a "software solution," and while parties can then be identified and one an know upon whom liability would be placed, this would not be a trustworthy system.").

[316] *Blockchain for the automotive industry: cardossier community to establish association*, CARDOSSIER MEDIA RELEASE 2 (May 3, 2019), https://cardossier.ch/wp-content/uploads/2019/03/mm_cardossier_association_20190306_en.pdf.

[317] *Id.*

[318] Otto C. Frommelt, Presentation, Governance of Blockchain projects across organizations and states: A case study of a vehicle's lifecycle with Blockchain technology (Nov. 19, 2019).

[319] CARDOSSIER, https://cardossier.ch/ (last visited Feb. 18, 2020).

or a well-known company known for best practices increases trust within the system and sets standards of best practice. Especially when a code is implemented in the system by which the actors must abide, examples of best practice can be followed. In essence, in a permissioned system, one can introduce responsible actors and regulate them within the system. While this represents a subset of the blockchain system as a whole, this example shows that actors within the system can be held accountable, and best practices can be ensured through a functioning code of conduct.

iii. Permissioned Layers

A final consideration is the introduction of permissioned layers. A permissioned layer is distinguished from a permissioned system and can act as a security measure to engage in the system. If one considers the "Ethereum blockchain, which is completely decentralized," one could introduce a layer via smart contract that would only allow interaction "with permissioned counterparties, so only with KYC approved counterparties." Thus, one can "use a good system that is completely decentralized," and combine this with a "KYC/AML compliant layer."[320] In that sense, one has a general understanding of the characteristics of the parties one is interacting with. The fact that these counterparties would have to respect certain standards would lower the liability risk in the ecosystem. It would also be easier to identify an accountable party.

B. Sub-Meta-level: Smart Contracts and Legal Smart Contracts

1. Pre-Defined Functions

As previously mentioned, the liability challenges of smart contracts stem from the interaction of pseudonymous parties. The first solution proposed is that of introducing a sort of arbitral tribunal ("Schiedsstelle"), which would be programmed as a function on the smart contract. This arbitral tribunal would rule over mistakes that could have occurred on-chain, such as programming errors. Additionally, it could rule over mistakes that occurred as off-chain events through oracles, which are web services connecting actions in the "real world" to the on-chain world and can thus communicate information that occurred off-chain. A platform provider such as Ethereum could even include an arbitral tribunal as an automatic, standard function within each smart contract.[321] The second solution proposed is to include a predefined function that would allow the parties to terminate and rescind the contract ("Beendigung

---

320 Interview with Mauro Casellini, CEO, Bitcoin Suisse AG (Sept. 23, 2019).

321 Smets, *supra* note 125, at 134.

und Rückabwicklung der Leistungen"), which would be automatically activated if certain events occur.[322]

2. Permissioned Layers

As the discussion on permissioned layers demonstrated, these layers could also be helpful in addressing the problem of pseudonymous counterparties. Having permissioned layers would enhance the trust in the system and ensure that the counterparty with which one is engaging is, for example, KYC compliant. This is linked to the liability gap in that then, one could identify a counterparty and thus enforce a liability claim.

CONCLUSION

The scenarios considered (first meta-level: the blockchain system as whole, and the sub-meta-levels considering two specific scenarios in the blockchain ecosystem: a smart contract, and a transaction over the blockchain system) touched upon different parts of the blockchain ecosystem and showed that there are liability gaps within each situation considered. In the first scenario, regarding the blockchain system as a whole, one could identify the challenges in regulating the entire blockchain system. The Blockchain Act provided the first real example of imposing liability upon actors within the system. However, the regulation of the actors within the system does not equate to a regulation of the underlying system as a whole. Regulating the entire system proves to be difficult to enforce. The discussion has indicated that it is sometimes difficult to identify responsible actors, or that it may not be possible to support the claims brought up by millions of individuals. In light of this, considering the blockchain system as a legal entity with separate personality is helpful, as this allows for the identification of a new model upon which liability attribution can be based. This could retain the current model in which developers are shielded by claiming compensation from the entity itself instead of from individual players. However, this could allow individuals to hide behind the corporate shield. Furthermore, the participants of this ecosystem could have a stake in the "entity" (which would be the blockchain), which in itself could even provide the basis for a form of compensation. It could also take on the form of a liability insurance scheme, depending on how one characterizes the blockchain system and how one defines key actors within the system. These considerations are in essence problematic, as they tend to go against fundamental principles of the blockchain system itself. Ultimately, it is individual actors who are responsible for the system, and whom liability would

---

322 *Id.*

have to fall back upon. Thus, different solutions may have to be taken into account altogether in order to provide a comprehensive liability basis. This may even allow for a respect of the fundamental principles upon which the blockchain system is based; features such as transparency and decentralization could be maintained while still ensuring that the individual actors behave accordingly.

For the specific scenarios (sub-metal levels) that were considered, the liability gap was effectively closed. Liability challenges relating to smart contracts and legal smart contracts were solved by applying the civil law basis. Technical problems arising from pseudonymous parties could also be mitigated through due diligence standards and the possible application of permissioned layers. The Blockchain Act honed in on the challenges presented by the decentralized nature of the technology and introduced middlemen into the system, while still not altering the underlying technology. In doing so, the best of two worlds was ensured: a decentralized system was maintained, and the legal certainty ensured trust in the system.

It remains to be seen how the token economy will further evolve and what ramifications this will have on the blockchain ecosystem. While the ecosystem will now adapt in response to the Blockchain Law and the newly created actors, the law must also continue to adapt and respond as the system continues to develop. The Civil Code and the addition of the Blockchain Act provide a great foundation that gives legal certainty to actors, as they know which parties can be held liable within the system and have assurance that their claims can be enforced in a court of law.

LIST OF ABBREVIATIONS

AT-ABGB	Allgemeines bürgerliches Gesetzbuch für die gesammten deutschen Erbländer der Österreichischen Monarchie (JGS Nr. 946/1811) in geänderter Fassung) Austrian Civil Code
AML	Anti-Money Laundering
Art.	Article
CFTC	Commodity Futures Trading Commission
CJEU	Court of Justice of the European Union
ECG	Gesetz vom 16. April 2003 über den elektronischen Geschäftsverkehr (E-Commerce-Gesetz) (LR 215.211.7) E-Commerce Law
EEA	European Economic Area
ERC-20	Token on Ethereum Platform
EU	European Union
FL-ABGB	Liechtenstein Civil Code (Allgemeines bürgerliches Gesetzbuch vom 1. Juni 1811) Liechtenstein Civil Code
GDPR	General Data Protection Regulation
ICJ	International Court of Justice
ICO	Initial Coin Offering
KYC	Know Your Customer
Lit.	Litera
Para.	Paragraph
PGR	Das Personen- und Gesellschaftsrecht vom 20 Januar 1926 (LR 216) Person and Companies Act

PrHG	Gesetz vom 12. November 1992 über die Produktehaftpflicht (Produktehaftpflichtgesetz) (LR 215.112.2) Product Liability Law
SEC	Securities and Exchange Commission
SPG	Gesetz vom 11. Dezember 2008 über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz) (LR 952.1) translated as Due Diligence Act
TCM	Token Container Model
TT	Trusted Technology
TVTG	Gesetz vom 3. Oktober 2019 über Token und VT-Dienstleister (Token- und VT-Dienstleister-Gesetz) (LR 950.6) Token And Trusted Technology Service Provider Act
U.S.	United States of America