

Eleonor Gyr

Smart Contracts and Contract Law

Smart Contracts sind nun seit geraumer Zeit ein Thema, das auch Juristen beschäftigt. Dabei kommt regelmässig die Frage auf, ob ein Smart Contract für sich alleine auch einen gültigen Vertrag darstellen kann. Dieser Frage geht der vorliegende Artikel nach, wobei auf Grundprinzipien des Schweizer Vertragsrecht eingegangen wird.

Category of articles: Blockchain

Region: Switzerland

Field of law: Blockchain

Collection: Conference proceedings IRIS 2022

Citation: Eleonor Gyr, Smart Contracts and Contract Law, in: Jusletter IT 30 June 2022

Contents

- Introduction
- 1. Smart Contracts
 - 1.1. Characteristics and Mechanism
 - 1.2. Conditions Set in the Smart Contract
- 2. Legal and Contractual Capacity of the Contracting Parties
 - 2.1. Legal and Contractual Capacity According to Civil Law
 - 2.2. Determination of Legal and Contractual Capacity in Relation to Smart Contracts
- 3. Declaration and Attributability of the Declaration of Intent
 - 3.1. Declaration of Intent
 - 3.1.1. General
 - 3.1.2. In Electronic Legal Transactions
 - 3.1.3. With Smart Contracts
 - a. Qualified Person
 - b. Unqualified Person
 - c. Qualified and Unqualified Person
 - 3.2. Attributability of the Declaration of Intent
 - 3.3. Conclusion
- 4. Programming Language as a Contract Language
 - 4.1. Freedom of Form
 - 4.2. Programming Language
 - 4.3. Programming Language as a Contractual Language
- 5. Formal Requirements
 - 5.1. Simple Written Form
 - 5.1.1. Declaration Content in Characters (Erklärungsinhalt in Schriftzeichen)
 - a. Declaration content in characters in e-commerce transactions
 - b. Declaration Content in Characters in Smart Contracts
 - 5.1.2. Declaration Medium
 - a. Declaration Medium in e-Commerce Transactions
 - b. Smart Contract as Declaration Medium
 - 5.1.3. Signature
 - a. Signature in e-Commerce Transactions
 - b. Signature with Smart Contracts
 - 5.1.4. Preliminary Conclusion
 - 5.2. Qualified Written Form
 - 5.3. Public Certification
 - 5.4. Consequences of Formal Invalidity
 - 5.4.1. Nullity and Partial Nullity
 - 5.4.2. Reversal and Conversion
 - 5.5. Conclusion
- 6. Summary and Outlook
- 7. References

Introduction

[1] Due to the increasing awareness and widespread use of blockchain technology (and thus also of smart contracts), the phrase «Code is Law», coined by the US jurist Lawrence Lessing, has become a popular catchphrase – a fact illustrated by this paper’s title and a rich abundance of technical articles citing the expression.

[2] The driving element and actual conceptual innovation of blockchain technology is «built-in» trust: the blockchain has created a system that does not require the trust of the parties, which is why it is also called a trustless system. In fact, one of the underlying ideas of blockchain

technology is to overcome the trust aspect, which plays a central role in everyday economic life. We conclude contracts with parties of whom we assume that they shall honor what they have agreed to. This trust can be based on a party's reputation, government supervision or personal acquaintance. The trust aspect also plays a vital role in the legal realm, especially in private law. Consider, for example, the principle of good faith, which is found in a multitude of jurisdictions (for Swiss law see art. 5 para. 3 of the Federal Constitution; EPINEY 2015, art. 5 n 1 pp.; HONSELL 2018, art. 2 n 4.; for the USA cf. KCLASS 2010, 40; for England cf. PEEL 2020, 2; overview of the various jurisdictions in continental Europe with further references ZIMMERMANN/WHITTAKER 2000, 18 pp.).

[3] Due to the technical possibility of storing data in an unchangeable, decentralized and distributed manner, no counterparty needs to be trusted in a blockchain anymore; trust is solely technology-based. This represents a transfer of the trust aspect from established companies and institutions to a technology and thus a paradigm shift (on the trust aspect in the blockchain, cf. MOUGAYAR 2016, 29 pp.; SWANSON 2014, 16 p.; TAPSCOTT/TAPSCOTT 2016, 3 pp.). However, a closer look at the technology and its use cases reveals that while familiar intermediaries, such as banks, are no longer a vital necessity for certain actions or transactions, new intermediaries are required to make the technology usable by the masses (e.g. wallet providers or crypto exchanges). It can also be observed that established market players, particularly in the financial market, have adapted to the circumstances and have regained popularity as intermediaries; for example, some established financial intermediaries carry cryptocurrencies in their portfolios.¹

[4] Whether blockchain technology can also impact the basic principles of contract law is difficult to assess from today's perspective and is the subject of lively debate among academics, which explains the astounding number of recently published articles on the subject of smart contracts and contract law. What is certain, however, is that the automation of contracts based on blockchain technology, i.e. smart contracts, will lead to a solidification of the *pacta sunt servanda* principle (anchored in continental European civil law).²

[5] One specificity of smart contracts is their immutability and decentralized execution, a feature that has stirred up interest within the *FinTech* industry, in particular. In their application, smart contracts must therefore be checked against the «Code is Law» maxim, so as to provide an indication of whether they can be deemed as «real» contracts under the applicable rules of private law. To this end, it is paramount to consider the set of conditions required for a valid conclusion of a contract. As a Swiss lawyer, I base my observations on the principles of Swiss private law – assuming that Swiss law applies (for the determination of applicable law regarding smart contracts cf. KRAUS 2019, 66 pp.). However, these principles are very similar in many – at least continental European – jurisdictions due to their derivation from Roman law.³

[6] In the following text, many sources are technical articles that refer to Swiss (and partly German) law, which are mostly written in German. In jurisprudence, technical articles are still mostly

¹ For regulation of intermediaries in blockchain networks, cf.; ELLUL 2020, 209 pp.; EGGEN/SILLABER 2020; BRUMMER 2020, 134 pp.; FINK 2019, 55 pp.

² The *pacta sunt servanda* principle (contracts are to be respected) is firmly established in jurisdictions derived from Roman law. For a comparative legal view on smart contracts in the light of continental European civil and common law cf. FERENCZ, 2020.

³ For broader private law issues related to smart contracts, such as revocation of a declaration of intent, defects of intent, and liability for defective codes, cf. GYR 2019.

published in the national language. Wherever possible, however, English-language sources have been provided.

1. Smart Contracts

[7] The term *smart contract* was first used by Nick Szabo in his 1994 paper *Smart Contracts* (SZABO 1994). Szabo assumed as early as the 1990s that a mature (technical) security system would serve to process contracts automatically and that this would save costs in enforcing contracts (SZABO 1994, 1997). Today, the term smart contract is often used collectively for a range of applications.

[8] The Ethereum network plays a pioneering role when it comes to smart contracts. In fact, Ethereum calls certain codes that can be initiated on the Ethereum blockchain *smart contracts* and describes their function as follows: «*Smart contracts are a type of Ethereum account. This means they have a balance and they can send transactions over the network. However, they are not controlled by a user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible.*» (<https://ethereum.org/en/developers/docs/smart-contracts/>).

[9] The Ethereum smart contract has been explicitly referenced in this chapter due to its significance for the blockchain community. Undoubtedly, Ethereum has played a pioneering role in the field of smart contracts. Although the term was adopted and re-defined by the Ethereum platform, it has since become a general term detached from the Ethereum project.

[10] The multitude of definitions in circulation can be boiled down to the essence that a smart contract is a piece of software that can be executed on a blockchain platform, involving at least two parties, and where assets are transferred according to predefined conditions (definition approaches in TIMMERMANN 2020, 71 pp.; SCHÄR/BERENTSEN 2020, 228 pp.; BAL 2019, 12 p.; WEBER 2018 2, 704; BACON/BAZINAS 2017, n 3; MOUGAYAR 2016, 42 p.; CLACK et al. 2016, 2; SWANSON 2014, 16, SWAN 2015, 16).

1.1. Characteristics and Mechanism

[11] A smart contract can be stored directly on a blockchain (as a state). In the case of the Ethereum blockchain, for example, the smart contract is implemented as a contract account on the blockchain (cf. SCHÄR/BERENTSEN 2020, 229; MIELKE/WOLFF 2018, 3 p.; PLOOM 2016, 129). Because it is stored directly on the blockchain, the smart contract cannot be modified subsequently. The resulting transaction carried out by the smart contract can be checked and validated by the nodes at any time, which suggests a secure outcome (cf. PLOOM 2016, 129; MIELKE/WOLFF 2018, 4; FURRER 2018, 104.). The direct anchoring of the smart contract to the blockchain is certainly an advantage in terms of tamper resistance as well as validation of the transaction by the network; however, in the case of faulty⁴ smart contracts, it represents a disadvantage due to its immutabil-

⁴ Faulty in the sense that the smart contract does not execute what the parties actually intended, whether due to incorrect programming or lack of will on the part of the parties.

ity. Likewise, the direct storage of the smart contract requires immense storage capacity and computing power in the network, since each node executes the smart contract and the result, i.e., the transaction, is validated over and over again (PLOOM 2016, 129, 144).

[12] In addition to storing the smart contract as a state on the blockchain, it is also possible to store it outside the blockchain, e.g. in a virtual container (cloud), or to only store the hash of the smart contract and/or only the result of the smart contract in the blockchain. This model has been developed especially for private applications and companies, as such a model allows the smart contract to access systems of companies and does not require much storage space on the blockchain (e.g., Chaincode by HYPERLEDGER; cf. PLOOM 2016, 144). Also, resorting to external storage enables the parties to intervene (e.g. in the event of faulty programming or altered circumstances).

[13] The mechanism relies on the principle that, in a smart contract, the assets contributed by the parties are automatically distributed according to the rules agreed upon by the parties, referring to data yet unknown at the time of smart contract initiation.

1.2. Conditions Set in the Smart Contract

[14] As smart contracts reference data unavailable at the time of initiation, they contain conditions. This information can either be stored on the blockchain (so-called *on chain*) or linked to an event or piece of data outside the blockchain (so-called *off chain*), either in the virtual or real world. The reference to information outside the blockchain can be established by a so-called *oracle*. The oracle is a third party, a trusted entity chosen by the parties, which, for example, stores the occurrence of a certain event as a transaction in the blockchain, which in turn is referenced by the smart contract. Alternatively, the oracle holds a private key that is assumed to be a condition for triggering the transaction (cf. COSTANTINI et al. 2021, 89 p.; SCHÄR/BERENTSEN 2020, 232; SWAN 2015, 17; SWANSON 2014, 61; WEBER 2017, N 33 p.).⁵ It should be noted here that these interfaces pose a certain security risk because they can block assets depending on their programming and the information carried into the blockchain from the outside is not validated by the network (cf. MIK 2017, 9; for problems and possible solutions when using oracles cf. SCHÄR/BERENTSEN 2020, 232).

2. Legal and Contractual Capacity of the Contracting Parties

[15] A smart contract requires the involvement of at least two parties (see chapter 1). A basic prerequisite for the conclusion of a contract is thereby met by smart contracts, since, under civil law, the conclusion of a contract invariably requires the involvement of more than one party; a contract cannot be concluded with oneself.

⁵ The connection from a smart contract to an object in the real world can also be established by means of interfaces to the Internet of Things (IoT; on the connection between blockchain and IoT cf. TRILLMICH et al. (2020), 174 p.; CHRISTIDIS/DEVETSIKIOTIS 2016, 2298 pp.). IoT is an Internet-based information architecture that enables real objects to communicate with the virtual world using built-in microcomputers (EGGEN 2016, 1131 p.; WEBER/WEBER 2009, 1).

[16] As an additional requirement, the involved parties must possess legal capacity (*Rechtsfähigkeit*) for a contract to be deemed *valid*; these prerequisites are indispensable (for Swiss law: cf. BERGER 2018, n 300, 305; GAUCH et al. 2020, n 299 p.).

[17] If the parties wish to ensure that the conclusion of the contract does not subsequently prove to be invalid due to lack of legal capacity, this aspect ought to be verified prior to contract conclusion. As a rule, this is done by identifying the contracting parties. In practice, the aforementioned requirements are not checked separately, but rather collectively; in fact, age and identity are usually the only elements disclosed or checked for most legal transactions.

2.1. Legal and Contractual Capacity According to Civil Law

[18] In Switzerland, all natural and legal persons possess legal capacity by law (art. 11 and 53 Swiss Civil Code (CC); GAUCH et al. 2020, n 300; HÜRLIMANN-KAUP/SCHMID 2016, n 566 pp.; HOFER/HRUBESCH-MILLAUER 2012, n 11.03 p.). Legal capacity is therefore presumed and begins with completed birth and ends with death. Any limitations of it must be proven by the party intending to derive any benefit therefrom (STEINAUER/FOUNTOULAKIS 2014, n 40 p.; cf. HOFER/HRUBESCH-MILLAUER 2012, n 11.07, 11.11).

[19] In addition to legal capacity, contractual capacity (*Geschäftsfähigkeit*) is also required for the valid conclusion of a contract. Contractual capacity (along with the responsibility for torts [*Deliktsfähigkeit*]) is a subtype of the capacity to act (*Handlungsfähigkeit*, art. 12 CC for natural persons, art. 54 CC for legal persons) and refers to the capacity of a person to make declarations of intent in legal transactions (HOFER/HRUBESCH-MILLAUER 2012, n 10.14; HUGUENIN 2019, n 142; HÜRLIMANN-KAUP/SCHMID 2016, n 591). Capacity to act is indispensable for both bilateral and unilateral legal transactions (*Rechtsgeschäfte*) and the rights and obligations emanate from it (HOFER/HRUBESCH-MILLAUER 2012, n 10.14; HÜRLIMANN-KAUP/SCHMID 2016, n 590 pp.; FANKHAUSER 2018, art. 12 n 12 p.).

[20] Natural persons must be of age⁶, capable of judgment⁷ and must not be under general deputyship (*umfassende Beistandschaft*)^{8,9}. Legal persons are capable of acting once the necessary bodies have been appointed in accordance with the law and the articles of association (art. 54 CC). Unlike legal capacity, capacity to act is not presumed.¹⁰

⁶ In Switzerland, a person is considered to be of age when they reach the age of 18, art. 14 CC.

⁷ According to Swiss law, a person is capable of judgement if they are able to act rationally, i.e. if they are not limited in their ability to act rationally due to childhood, mental disability, mental disorder, intoxication or similar conditions, art. 16 CC.

⁸ General deputyship is ordered in Switzerland if the person concerned is permanently incapacitated and in need of special assistance; said person's capacity to act ceases by law, art. 17 CC.

⁹ Even persons with limited capacity to act (e.g. persons incapable of judgment, art. 19–19c CC) can be partially capable of contracting and can conclude certain legal transactions with legal effect (art. 19 para. 1 and 2 CC; cf. BERGER 2018, n 322; HOFER/HRUBESCH-MILLAUER 2012, n 10.26 pp.; HÜRLIMANN-KAUP/SCHMID 2016, n 597 pp.). The lack of contractual capacity as a consequence of the lack of capacity of judgement causes the contract to be void. If, on the other hand, a person capable of judgement lacks the presupposed capacity to act, the contract is considered non-binding for that person without the consent of their legal representative (BERGER 2018, n 311 p.; GAUCH et al. 2020, n 302; HOFER/HRUBESCH-MILLAUER 2012, n 10.40).

¹⁰ It should be noted that in Switzerland, among other countries, good faith regarding the capacity to act is not legally protected (Federal Court Decision [BGE] 107 II 105 deliberation 6a p. 116, 89 II 387 deliberation 2 p. 389; BERGER 2018, n 319; GAUCH et al. 2020, n 301).

[21] The consequence of the lack of a contracting party's legal capacity is the nullity or unilateral non-binding character of the contract.

[22] Nullity means that no contractual effect takes place (BGE 4C.163/2002 of July 9, 2003 deliberation 1.3; BGE 134 III 438 deliberation 2.3 p. 442 p.; GAUCH et al. 2020, n 681). According to prevailing Swiss doctrine, the contract is invalid *ex tunc* and any service under the void contract therefore lacks a valid legal basis (BERGER 2018, n 1103; GAUCH et al. 2020, n 681; HUGUENIN/MEISE 2015, art. 19/20 n 53; SCHWENZER 2020, n 32.35; BGE 134 III 438 deliberation 2.3 p. 442 p.). Accordingly, nullity can be asserted by anyone and the court has to consider nullity *ex officio*, provided that a ground for nullity arises from the party's submission (BUCHER 1988, 241 p.; GAUCH et al. 2020, n 681; HUGUENIN/MEISE 2015, art. 19/20 n 53; KRAMER 1991, art. 19–20 n 308 pp.). If service has already occurred, then, in accordance with the provisions applicable under the given circumstances, there is the possibility of a vindication in the case of real property (art. 641 para. 2 CC) or a claim for unjust enrichment (art. 62 pp. Code of Obligations [CO]). Action to correct the land register may also be considered (art. 975 CC; cf. SCHMID 2019, art. 975 n 1 pp.).

2.2. Determination of Legal and Contractual Capacity in Relation to Smart Contracts

[23] As outlined above, a smart contract can be implemented in a blockchain in different ways. As long as the smart contract is only used as a tool for enforcing a contract, the determination of legal capacity plays a subordinate role, as this validation is (or should be) ensured in the underlying transaction outside the blockchain. The question of parties' legal and contractual capacity deserves special attention in cases where smart contracts are designed to directly represent the underlying transaction. From a practical point of view, the question of party identification is key as far as public blockchains are concerned (in the case of closed blockchain networks, identification may be part of the admission requirements).

[24] One key principle of a public blockchain is its universal accessibility. Since a public blockchain is generally accessible to everyone and does not require a central instance, any form of admission control (e.g. only those who identify themselves are admitted) is not realistic and counter-acts its fundamental concept. It is therefore the responsibility of the potential contracting parties to verify the legal and contractual capacity of their contracting parties outside the blockchain or to demand proof of the latter. One possibility includes the use of an application for the contract conclusion to ensure identification of the parties and verification or proof of the contracting parties' legal capacity, respectively.

[25] If contracts are concluded on a private or closed blockchain, participant identification can be provided for from the outset. This means that only participants who can prove their legal capacity or identify themselves in advance are admitted to the blockchain. The proof-of-identity design is contingent on the rules of the blockchain or the application. However, even in the case of a private blockchain, it is up to the individual users whether and how they obtain proof of the legal capacity of their contractual partner.

[26] It is self-evident that the general legal consequences set out above caused by the absence of legal capacity (nullity, unilateral non-binding character) also apply to any invalid contracts executed as smart contracts. In this constellation, however, there is an additional element that com-

plicates matters: if the smart contract is stored directly on the blockchain, then the smart contract itself as well as its result (transaction) are basically irrevocable and unchangeably stored. The invalidity of a smart contract or a transaction cannot be recorded in a blockchain (cf. WEBER 2019, 306; CARRON/BOTTERON 2019, 115 pp.). Furthermore, this would contradict the basic principle according to which a result is considered valid if the predefined conditions are met. Modification of a smart contract would only be conceivable in cases where the smart contract is stored in a virtual container outside the blockchain and the result has not yet been stored in the blockchain. In a closed system, one could theoretically define the rule that a transaction can be marked as invalid in retrospect; however, this would plunge the entire system into considerable legal uncertainty and take the fundamental concept and advantages of blockchain technology ad absurdum.

[27] Therefore, a certain degree of legal uncertainty already exists at the time of contract conclusion if the parties do not sufficiently identify each other or do not provide proof of legal capacity.¹¹ A key principle of blockchain technology, however, is that the information written in the blockchain is assumed to be correct and trustworthy. With regard to the above, technology undermines the law. If it is clear which law governs a given contractual relationship, the principle of good faith must be analyzed under the corresponding set of rules to establish whether the subsequent transactions of an originally invalid transaction could nevertheless be deemed effective (in legal terms, not just on the blockchain).

3. Declaration and Attributability of the Declaration of Intent

[28] For a contract to become effective, not only must there be several contracting parties possessing legal capacity (see chapter 2 above), but also a consensus of the parties to establish a contractual relationship together (there must be consensus at least on the *essentialia negotii*).¹² In connection with smart contracts, the question arises as to whether a declaration of intent «expressed» by means of smart contracts can at all be understood and attributed as an expression of the will of a party.

3.1. Declaration of Intent

3.1.1. General

[29] Under Swiss law, establishing a contract requires a concurring mutual declaration of intent (art. 1 para. 1 CO). This consent may be express or implied (art. 1 para. 2 CO). Whereas the chronologically first declaration of intent represents the proposal, the second represents acceptance (BERGER 2018, n 647, 668; GAUCH et.al 2020, n 363 pp.; SCHWENZER 2020, n 28.01; WEBER 2010, 340).

[30] With the proposal, the applicants declare their final intention to conclude a contract (BERGER 2018, n 648; GAUCH et al. 2020, n 363; SCHWENZER 2020, n 28.09). This is to be distinguished

¹¹ In fact, legal capacity plays a minor role, since it is assumed in the case of natural persons from birth, and in the absence of legal capacity of a legal person, the natural person establishing the contractual relationship on behalf of the legal person becomes obligated.

¹² For the requirements of a valid contract under common law, cf. BUGG (2020).

from the invitation to make an offer (*invitatio ad offerendum*), which may be addressed to one or more persons and with which only the willingness to conclude a contract – but without a final intention to conclude – is declared (BERGER 2018, n 648; GAUCH et al. 2020, n 369; cf. SCHWENZER 2020, n 28.09).

[31] Legal intent (the intention to establish legal relations and recognize their consequences) is the result of a mental effort consisting in both parties weighing the different aspirations and obtaining a point of view with which one is willing to be bound (ZELLWEGER-GUTKNECHT/BUCHER 2015, art. 1 n 3). The existence of a will to be bound is elementary for distinguishing a contract from a courtesy (GAUCH et al. 2020, n 353a; cf. HÜRLIMANN-KAUP 1999, n 110). If the will is interpreted according to the principle of trust, then a binding will is denied in the case of courtesy and commitments in a purely social context (GAUCH et al. 2020, n 353b w.f.r. HÜRLIMANN-KAUP 1999, n 116).

[32] Acceptance is the manifestation of the intention to conclude a contract and, as a second declaration of intent, must be consistent with the proposal – if its content deviates from the offer, this is generally deemed to be a counteroffer (BERGER 2018, n 670; GAUCH et al. 2020, n 435, 441; SCHWENZER 2016, n 28.31).

3.1.2. In Electronic Legal Transactions

[33] In e-commerce, too, there must be an intention to be legally bound in order for a contract to be valid. In the early days of e-commerce, it seemed questionable whether users were aware of the point in time they concluded a contract by means of a click, due to the countless mouse clicks required. In the meantime, it has been recognized that a mouse click is attributed to the sender (see chapter 3.2 below). Due to regulatory requirements, among other things, websites are designed in such a way that explicit reference must be made to the fact that a contractual relationship is being established.¹³ It is therefore unlikely that a legal relationship will be established by chance without the intention of becoming legally bound.

3.1.3. With Smart Contracts

[34] In cases where a smart contract is used to represent and/or enforce a contract concluded outside the blockchain, the intention to be legally bound must occur in this underlying transaction. The intention to engage in a transaction only needs to relate to the use of the smart contract (e.g., as a representation or enforcement tool) if the use of the smart contract reflects a key point of the contract (cf. FURRER 2018, 106; WEBER 2018 1, 293).

[35] In other cases, i.e. if the smart contract itself is designed to constitute the contract, it must be differentiated whether the parties involved are qualified persons able to understand the essential regulations in the smart contract (e.g. by mastering the programming language¹⁴), whether it is

¹³ See, for example, for the European Union (EU), art. 11 Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular e-commerce, in the Internal Market (OJ, L 178/1).

¹⁴ For programming language as a contract language, see chapter 4.

possible for both parties to understand the content of a smart contract in a just and reasonable manner or whether the parties have diverging levels of understanding.¹⁵

a. Qualified Person

[36] If qualified parties use a smart contract without first concluding another contract, it can be assumed that the use of the smart contract and the conditions contained therein correspond to the will of the parties. Since a programming language can, in principle, be a contract language (see chapter 4 below), in this constellation the smart contract (assuming the other requirements for a valid contract conclusion are met) directly represents the contract.¹⁶ As a smart contract refers to information (events) that is not yet known at the time of contract conclusion, it is usually a (resolutive or suspensive) conditional contract.¹⁷ A conditional contract can be used for almost all legal transactions due to the private autonomy enshrined in Swiss law (EHRAT/WIDMER 2015, preliminary remarks art. 151–157 n 4; BERGER 2018, n 790; GAUCH et al. 2020, n 3952). However, legal transactions that lead to an unacceptable impairment of legal certainty or contain an unlawful or immoral intention cannot be subject to conditions (EHRAT/WIDMER 2015, preliminary remarks art. 151–157 n 5a; BERGER 2018, n 794 p.).

b. Unqualified Person

[37] Although blockchain technology is becoming increasingly popular, from today's perspective the scenario of an unqualified person implementing a smart contract «by mistake» is rather unlikely. Initiating a smart contract on a blockchain and transferring assets to the address of the smart contract always requires an action on the part of at least one party. This action can also attribute an intention to act to the party. Whether this action also includes a business intention can only be assessed on a case-by-case basis. What is certain, however, is that by signing with their private key, parties consciously trigger a transaction.

[38] Should parties be unaware of the scope of the signed transaction (or incapable of reasonably understanding the contents of the smart contract due to a lack of knowledge) and there is no intention to be bound with the associated (legal) consequences, then the smart contract itself does not constitute a contract. In this constellation, however, it is questionable whether the parties should be precluded from invoking the lack of the intention to engage in a transaction in the case of conscious use of a smart contract without knowledge of the specific content (as manifest abuse of a right [*Rechtsmissbrauch*] is not protected by Swiss law; cf. WEBER 2017, n 10; on the abuse of a right HAUSHEER/AEBI-MÜLLER 2012, art. 2 n 41 pp.; on the described constellation in German law KAULARTZ/HECKMANN 2016, 624).

¹⁵ CARRON/BOTTERON (2019, 124) do not differentiate between qualified and unqualified persons and assert that an offer can be written in computer code, for all intents and purposes.

¹⁶ SCHALLER (2018) takes a different view, arguing that the contract is concluded «one legal second» beforehand: The parties conclude the contract in writing, verbally or implicitly in advance and only then convert it into a smart contract; unless the parties explicitly declared that they did not want to be bound until the contract was available as a smart contract. This opinion must be contradicted insofar as this would also have to apply consistently to contracts concluded without smart contracts: In the case of a written contract, the contract is not usually concluded verbally or implicitly in advance; rather, this is the stage of the pre-contractual negotiations.

¹⁷ According to art. 151 para. 1 CO, the condition is the occurrence of an uncertain fact; it stands for an objectively uncertain future event on which, according to the will of the parties, the validity of the contract depends; cf. EHRAT/WIDMER 2015, preliminary remarks art. 151–157 n 1.

c. Qualified and Unqualified Person

[39] If a contract is drawn up with a smart contract and the parties involved are a qualified and an unqualified person, the situation needs to be assessed on a case-by-case basis. If the unqualified person is a consumer¹⁸ and the qualified person is a company, it must be assumed that the smart contract does not represent the contract itself due to the lack of translation of the contract into natural language (see chapter 4 below).¹⁹ If it is not a consumer contract, then the intention of the unqualified person must be considered. If it was reasonably possible for the unqualified person to fathom the content of the smart contract (e.g. by inquiring with the contracting party), then the smart contract itself constitutes the contract – provided that the other requirements for the valid conclusion of the contract are met.

3.2. Attributability of the Declaration of Intent

[40] A declaration of intent must be attributable to one party. The imputability of declarations of intent plays a role in particular where a person other than the contracting party itself is involved in the conclusion of the contract, such as is the case with a messenger or representative.

[41] Since the Internet became accessible to the general public in the mid-1990s, thus heralding the advent of e-commerce, the dogmatic classification and attribution of so-called «electronic» declarations of intent has been thoroughly examined. A distinction is still made between those declarations that are made by a human being using a computer (e.g., by clicking a button), the so-called automated declarations of intent, and those that are generated automatically by a computer program, the so-called computer declarations (SPECHT-RIEMENSCHNEIDER 2020, 270 p.; BALSCHKEIT 2005, 168; WETTIG/ZEHENDNER 2004, 120 pp.; WEBER/JÖHRI 2000, 48). The former can be directly attributed to the sender (BALSCHKEIT 2005, 168; WEBER/JÖHRI 2000, 48). The declarations generated by a computer program are predetermined; in contrast to the first group of cases, doctrine holds that these declarations are not directly triggered by human action; a machine takes the legally relevant action (BALSCHKEIT 2005, 168; WEBER 2010, 340; WEBER/JÖHRI 2000, 49). As a result, however, this (computer) act is attributed to the operator of the corresponding data processing system (WEINGART 2020, 702, 704; WEBER 2010, 340; BALSCHKEIT 2005, 168 p.; for German law, cf. SPECHT-RIEMENSCHNEIDER 2020, 270 p.; HOEREN 2018, n 737).

[42] It is debatable whether the above distinctions between electronic declarations of intent (still) make sense. In principle, a person's declaration of intent is expressed either immediately or subsequent with the aid of a computer. These actions or expressions are always based on a software – depending on what is intended, the software will then trigger the declaration immediately or with a delay, because a condition or an acceptance of the offer has to occur first. According to the

¹⁸ A consumer is a natural person who acquires goods or services for personal or family use (KRAMER et al. 2016, 62; cf. art. 40a para. 1 CO, art. 32 para. 2 Civil Procedure Code [CCP], art. 120 para. 1 Federal Act on International Private Law [PILA] or art. 15 para. 1 Lugano Agreement); for the concept of consumer in the EU, see art. 2 Directive 2011/83/EU of the European Parliament and of the Council of October 25, 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ, L 304/64).

¹⁹ According to Trillmich et al. (2020), German law also requires the identification of the contracting parties in consumer contracts.

opinion represented here, this immediate or delayed expression plays no role for the imputability of the declaration of intent; it always presupposes an original human action.

[43] In addition to this distinction, the term *electronic agent* (also called *software agent* or similar) has been introduced to refer to a program that autonomously performs tasks without depending on the continuous input or control of a human being. This definition has been more or less uniformly adopted by doctrine across countries and is also partly reflected in legislation, e.g., in the U.S. Uniform Electronic Transaction Act of 1999 (for a comparison of definitions in the U.S. and Canada with reference to German law, cf. WETTIG/ZEHENDNER 2004, 130; cf. WEINGART 2020, 701, KIANICKA 2012, 53). In analogy to the term smart contract, the adjective *smart* was already used for electronic agents. However, *smart* pointed to programming even then; the agent is as smart as the programming intended it to be. An electronic agent is therefore simply software. With regards to electronic agents, it has been discussed whether they have or should have independent legal personality due to their suggested artificial intelligence. This has been largely denied, since the actions of an electronic agent can also be attributed to a person (for a detailed discussion of this topic with comparative legal aspects, cf. WETTIG/ZEHENDNER 2004; cf. KIANICKA 2012, 63 pp.).

[44] A discussion similar to that on electronic agents now revolves around smart contracts. The doctrinal classification of smart contracts is the subject of lively debate, with an assignment under the rules of agency, messenger or electronic agent being discussed in most cases (for German law: Weingart 2020; for Swiss law: FURRER 2018). Occasionally, there is also a plea for giving the smart contract its own legal personality (MEYER/SCHUPPLI 2017).

[45] A smart contract is always initialized by at least one party. This principle also applies to complex smart contract structures.²⁰ If a smart contract has been programmed to initiate further smart contracts itself, then this «action» is originally attributable to the programming of the first smart contract. It is possible to trace actions back to the initiating person based on the transaction history (cf. BAL 2019, 14). In doing so, a smart contract executes the steps that have been pre-programmed. These «actions» can therefore be assigned to the parties to whom the initialization or the associated data processing system can be attributed, just as with any other computer declaration or «electronic agent» (cf. MAUME et al. 2020, 145).

[46] The traceability of a smart contract to a party can also be achieved by verifying the transactions. If, for example, an asset is transferred to the address of the smart contract by the parties, this transaction is registered in the blockchain (publicly, if it is a public blockchain); by means of a signature, this transaction can be assigned to a party. However, the assignment is not to be confused with the identification of this party. In principle, pseudo-anonymity or pseudo-identity prevails in the blockchain. In the case of public blockchains, such as the Bitcoin or Ethereum blockchain, the participants do not have to identify themselves in order to participate in the network. Each participant in a blockchain is assigned a cryptographic key pair (or the participants select the key themselves), thereby also deriving one or more address(es) and creating a pseudo-identity (cf. SCHÄR/BERENTSEN 2020, 83 p., 88; SIXT 2017, 33). The addresses consist of a sequence of letters and numbers. Depending on the network, addresses are assigned per transaction or on an ongoing basis (SIXT 2017, 33; cf. for addresses in the Bitcoin blockchain in detail

²⁰ A complex smart contract entity is, for example, a decentralized autonomous organization (DAO). Cf. on the classification of «The DAO» in Swiss law GYR 2017; considerations on the DAO in German law w.f.r. RICHTER 2020, 150 p.; generally on the case of «The DAO» SHIER et al. 2017.

SCHÄR/BERENTSEN 2020, 88 pp.; ANTONOPOULOS 2015, 64 pp.).²¹ Often, in the context of public blockchains, identification occurs upon «entry» into the virtual world, for example, with the purchase of a cryptocurrency from a corresponding exchange or merchant, or upon «exit» when cryptocurrency is exchanged for fiat currency.²² The purchase and sale of virtual currencies is subject to money laundering regulations, i.e., the buyers or sellers of cryptocurrencies are identified by the dealers or exchanges (Swiss Federal Council 2014, 15; GRÜNEWALD 2015, 105 pp.; SIXT 2017, 33). Therefore, as soon as there is a connection between the real and the virtual world, identification is often unavoidable.²³ Even so-called mixer services, which are supposed to help Bitcoin users to disguise their true identity, do not offer conclusive protection in this respect. However, even if identification takes place, this does not mean that the identity of the other party to the smart contract is known. Overall, it can be stated that pseudo-anonymity exists, which should not be confused with «real» anonymity. From a global perspective, it is also possible to draw conclusions about the identity of users on public blockchains, but these do not necessarily have to be known to the parties to the smart contract.

3.3. Conclusion

[47] Assuming that a smart contract can itself constitute the contract, the initiation and also the transfer of assets to a smart contract can be understood as an expression of will and the action performed by the smart contract, constituting the transaction of assets according to predefined conditions, can be assigned to the parties involved in the smart contract. Attributability to a party must not be confused with the identification of the party.

4. Programming Language as a Contract Language

[48] With the automation of contracts, and especially in the context of smart contracts, the question arises whether a contract can also be written directly in programming language. Needless to say, this question is only of interest where there is no contract in any other (e.g. written) form.

4.1. Freedom of Form

[49] In principle, Swiss contract law, but also many other jurisdictions, do not impose formal requirements (see chapter 5 below). This means that the contract does not have to be set down in writing, nor does it have to be «linguistically produced» (HUGUENIN 2011, 114). According to HUGUENIN (2011, 114), the lack of language and form requirements for contracts has a long

²¹ If addresses are not changed for each transaction, there is a risk that transaction patterns can be elicited and the identity of a person can be inferred (SCHÄR/BERENTSEN 2020, 90; SIXT 2017, 33).

²² In order to avoid identification, specialized services exist, which offer an exchange into a fiat currency via a third party, e.g. <https://localbitcoins.com> (person in the vicinity exchanges Bitcoins into fiat currency and hands them over in cash to the client).

²³ With technical know-how, it is also possible to draw conclusions about the devices used, IP addresses, mail addresses or even the identity via assigned (blockchain) addresses (ISLER 2017, n 4; SIXT 2017, 155). Cf. study by researchers at the University of Luxembourg who examined a method for eliciting IP addresses from which Bitcoin transactions were generated: <https://arxiv.org/pdf/1405.7418.pdf>.

history. However, even if there is no need for language and form, a consensual mutual declaration of intent between the parties is needed (see chapter 3 above).

4.2. Programming Language

[50] Software is written in a certain programming language and is only readable/translatable by computers (and specialists in the field). Nowadays, so-called higher programming languages are commonly used, which no longer have to be de-coded directly by a computer, but are translated into machine language by a translation program (compiler) and are thus not only more problem-oriented, but also easier to understand (HEROLD et al. 2017, 148 p., 233; KRYPCZYK/BOCHKOR 2015, 5; cf. WEBER 2020, 501). Well-known (higher-level) programming languages include Java, C++ or JavaScript, Go, Python or Solidity, which are widely used in blockchain applications.

[51] In contrast to natural language (i.e. language spoken by humans), programming language can only represent syntax, but not semantics. Programming language consists of a sequence of characters, each of which has a specific function. It is therefore not possible to use programming language to represent indeterminate legal notions (cf. CARRON/BOTTERON 2019, 115; DE FILIPI/WRIGHT 2019, 77; WEBER 2017, n 18). From this point of view, one could argue that a fully worded contract cannot be drafted using programming language. But it should be kept in mind that even conventional contracts are often not comprehensively drafted nor free of contradictions (oral or tacit contracts are also to be considered here; cf. CARRON/BOTTERON 2019, 120). Unlike conventional language, programming language is not accessible to the general public,²⁴ but this could change in the future with technological change and the digitization of all areas of life.²⁵

4.3. Programming Language as a Contractual Language

[52] As already explained, a mutual concurring declaration of intent is a substantive prerequisite for the conclusion of a contract. Since under Swiss law a contract can also be concluded without being cast in language, drafting a contract in the form of a programming language should be generally considered possible, provided that this corresponds to the concurring will of the contracting parties (cf. WEBER 2020, 502; same view for German law: KAULARTZ/HECKMANN 2016, 621 p.; critical of contracts directly as code FERENCZ 2020, 596; MIK 2017, 15 pp.).

[53] A distinction must be made between this principle and the question of the suitability of a smart contract to reflect the actual intentions of the contracting parties (see chapter 3), to comply with any formal requirements (see chapter 5) or to be admissible as evidence in court.

[54] At this point, it should be mentioned that there have been serious efforts since the late 1990s to digitally record contracts, e.g. with Ricardian Contracts (GRIGG 2000; pictorial representation in MEYER/SCHUPPLI 2017, 207) or to develop legal programming languages that are supposed to record contracts in a legally correct way in algorithms. There are various projects

²⁴ Cf. FURRER (2017, 107), who argues that higher-level programming languages are basically comprehensible to interested laypersons.

²⁵ Cf. HAAPIO (2020) on the noticeable change of how contracts are generally written and presented, with further references to different projects regarding contractual automation tools and legal designing.

that deal with the elaboration of legal programming languages (so-called legal programming; cf. DE FILIPPI/WRIGHT 2019, 73 p.). According to current knowledge, however, none of these systems has yet become established.

5. Formal Requirements

[55] Despite the freedom of form enshrined in many countries' legal systems, there are different formal requirements for specific legal transactions. In Swiss law, formal requirements include simple written form, qualified written form and public certification. The purpose of formal requirements is to protect citizens from certain legal transactions; they constitute a protection against over-hasty decisions (*Übereilungsschutz*) and exercise a warning function while, at the same time, adding security to legal transactions (SCHWENZER/FOUNTOULAKIS 2020, art. 11 n 2).

5.1. Simple Written Form

[56] In Swiss law, simple written form requires the signature of all contracting parties (art. 13 CO). *Written form*, however, is not defined in the law as *such*. According to doctrine and case law, written form includes a declaration content (*Erklärungsinhalt*) in written characters, which is recorded on a declaration medium (*Erklärungsträger*) and permanently stored (BGE 120 V 74 deliberation 3a; cf. GAUCH et al. 2020, n 504; KRAMER/SCHMIDLIN, 1986, General Explanations on art. 12–15, n 3; SCHWENZER 2016, n 31.06). Simple written form is required, for example, for the assignment of claims (cession) according to art. 165 para. 1 CO.

5.1.1. Declaration Content in Characters (*Erklärungsinhalt in Schriftzeichen*)

[57] In Swiss doctrine, the requirement of written form is inextricably linked to the presence of a signature, as can be inferred from the wording of the law.²⁶ Accordingly, in analog times, letters and telegrams met the requirement of written form if the letter or the dispatch bore the signature of the sender (GAUCH et al. 2020, n 507). However, this alone says nothing about the content of the declaration in writing.

[58] Doctrine agrees that the technique and instrument used to produce the writing are irrelevant, provided that a permanent medium is guaranteed (GAUCH et al. 2020, n 509; HUGUENIN 2019, N 349; SCHWENZER/FOUNTOULAKIS 2020, art. 13 n 4; cf. KRAMER/SCHMIDLIN 1986, General Explanations on art. 12–15 n 5). The declaration content must therefore be suitable to be permanently stored on the declaration medium (SCHWENZER 2014, n 31.06). Or much rather, permanence refers to the appropriate medium for the declaration (see below) and not so much to the content of the declaration in characters.

[59] According to KRAMER/SCHMIDLIN (1986), the content's writing and language must be comprehensible at least to those persons who are to be protected by the formal requirement; if third-party interests are affected, the written text must be generally accessible and secret languages

²⁶ Art. 13 CO: A contract for which the written form is required by law must bear the signature of all persons who are to be bound by it.

or scripts do not meet the requirement of written character (KRAMER/SCHMIDLIN 1986, General Explanations on art. 12–15 n 5). Braille, shorthand or typewriting are also recognized as written characters (BUCHER 1988, 164). According to older legal doctrine, a magnetic tape or a punched tape, for example, did not meet the requirement of written form, since no signature could be placed on these carriers and the declaration could only be read with technical aids (BUCHER 1988, 164; KRAMER/SCHMIDLIN 1986, General Explanations on art. 12–15 n 4; Swiss criminal law is less strict with regard to technical aids in the context of official documents [*Urkunde*] in art. 110 para. 4 Swiss Criminal Code [StGB], cf. Boog 2019, art. 110 para. 4 N 10).

[60] In contrast to the (older) Code of Obligations, the (newer) Swiss Code of Civil Procedure and the Private International Law Act recognize the so-called textual form.²⁷ This requirement is less strict than that of simple written form, as no signature is required (GIRSBERGER 2017, art. 358 n 10; GRÄNICHER 2021, art. 178 n 11). The prerequisite for textual form is a written expression that allows for permanent proof of the declaration (HUGUENIN 2019, n 347). The text must be visually perceptible and physically reproducible whereby the technologies used are irrelevant (GIRSBERGER 2017, art. 358 n 7; GRÄNICHER 2021, art. 178 n 11). In this sense, voice mails or videoconferences do not meet the textual form requirement, since the sender's message has not been composed in text form, even in cases where a document may be available to the recipient as text thanks to speech recognition (DASSER 2021, art. 358 n 2; GRÄNICHER 2021, art. 178 n 13). This is in line with the prevailing doctrine, which does not recognize sound recordings as texts satisfying the requirement of written form (HUGUENIN 2019, N 349; KRAMER/SCHMIDLIN 1986, General Explanations on art. 12–15 n 4).

[61] If the textual form is supplemented with a signature, it becomes equivalent with simple written form. It is therefore conclusive to refer to the (more recent) doctrine on textual form to construe the requirements regarding the declaration content expressed in written characters. Thus, the requirement of visual perceptibility is also to be included in the assessment of the declaration content in characters. On the one hand, the latter is a technology-neutral feature and, on the other hand, it corresponds to the undisputed principle that the type of language, writing technique and writing device used are irrelevant.

a. Declaration content in characters in e-commerce transactions

[62] E-mails, web forms or other digital «documents» used in e-commerce transactions are generally produced in a language and script accessible to the general public; they are visually perceptible. Visual perceptibility is produced by technical aids, which, according to older doctrine, does not satisfy the requirement of written form. However, this opinion is no longer appropriate due to the economic reality of e-commerce and the technological aids used today in everyday life. The visualization of information (data of all kinds) by means of technical aids is now standard in everyday business as well as in private life. Digital transformation equally affects the business world and the private sphere. Therefore, the content of a declaration that can only be made perceptible with technical aids but is visually perceptible may well satisfy the requirement of the declaration content being expressed in written characters.

²⁷ In German law, textual form is a formal requirement enshrined in the German Civil Code (§126b) (TRILLMICH et al. 2020, 179).

b. Declaration Content in Characters in Smart Contracts

[63] If it is assumed that smart contracts can directly establish a contractual relationship, then the requirement of declaration content expressed in written characters being a visually perceptible text must also apply to smart contracts, whereby it is irrelevant whether or not technical aids be used to achieve visual perceptibility.

[64] If a contract is set up directly as a smart contract, then the contract language is a programming language (see chapter 4 above). At present, it is questionable whether a programming language satisfies the requirement of declaration content in written characters. Although a programming language is visually perceptible, it is not a text form accessible to the general public, i.e. generally understandable. According to current doctrine, however, it is sufficient for the writing and language to be accessible to the declaring parties; only if third-party interests are concerned must the language be accessible to the general public (KRAMER/SCHMIDLIN 1986, General Explanations on art. 12–15 n 5). Consequently, a declaration made directly by means of a programming language could at most satisfy the criterion of simple written form if the text is understood by the parties concerned (i.e. they understand the relevant programming language as qualified persons, see chapter 3.1.2. above), no third party interests are concerned and there are both a valid declaration medium (see chapter 5.1.2 below) and valid signatures (see chapter 5.1.3 below). Whether or not these cumulative requirements are met has to be established on a case-by-case basis. For example, assignments of claims under Swiss law should never be considered to be meeting the requirements, as third-party interests are invariably involved in these cases (under Swiss law, a claim can be assigned without the consent and knowledge of the debtor, art. 164 para. 1 CO, cf. GIRSBERGER/HERRMANN 2019, art. 164 n 5 pp.)

5.1.2. Declaration Medium

[65] According to the traditional interpretation, the declaration medium is a physical object classified as deed (*Urkunde*, not in the meaning of a «public» deed [*öffentliche Urkunde*]); deeds are assumed to be in paper form (GAUCH et al. 2020, n 504 pp.; SCHWENZER/FOUNTOULAKIS 2020, art. 13 n 3; SCHWENZER 2016, n 31.06; BUCHER 1988, 164; HUGUENIN 2019, n 349; KRAMER/SCHMIDLIN 1986, General Explanations on art. 12–15 n 4). Deeds serve as change-resistant storage media for the declaration content. Modern means of communication and electronic data carriers have regularly been denied this characteristic, not least because no signature could be placed under the content of the declaration, or because the electronic signature was not deemed equivalent to the handwritten signature (see overview of modern means of communication and doctrines in Switzerland SCHWENZER/FOUNTOULAKIS 2020, art. 13 n 14–14e).

[66] In the case of textual form, a requirement enshrined in more recent legislation, the content of the declaration must be physically reproducible; in this case, however, there is no restriction for the declaration medium to be a deed (cf. GRÄNICHER 2021, art. 178 n 11). Electronic storage and transmission is permitted with regard to textual form, provided that the recipient has the possibility of storage and the text does not remain exclusively with the sender (e.g. only on the sender's server or a third-party server to which only the sender has access, GRÄNICHER 2021, art. 178 n 13).

[67] In summarizing the doctrine on the declaration medium within the meaning of art. 13 CO as well as the more recent doctrine on textual form, it can be noted that the declaration medium must store the declaration content in a change-resistant and permanent manner and that it must

be possible to physically reproduce the declaration content at any time. If the latest doctrine on textual form is followed, then the declaration content does not necessarily have to be recorded on paper, but can also be stored on an electronic data carrier or transmitted by means of modern communication media, provided that the authenticity and integrity of the content can be guaranteed; for the latter, the additional requirement of a signature is needed (see chapter 5.1.3 below).

a. Declaration Medium in e-Commerce Transactions

[68] Recent doctrine has advocated for the acceptance of electronic records as declaration media, as there are technological methods to ensure that data cannot be changed at a later stage (SCHWENZER/FOUNTOULAKIS 2020, art. 13 n 14c; XOUDIS 2012, art. 13 n 6). This view is also corroborated by the fact that in Swiss law the qualified electronic signature has been treated as equivalent to a handwritten signature since 2005. An electronic signature would make no sense if the associated declaration and the declaration medium in digital form were not accepted (cf. HUGUENIN 2019, n 349; XOUDIS 2012, art. 13 n 6).

[69] In principle, a distinction must be made between the declaration medium itself and the form of transmission when considering the question of the declaration medium. There are two groups of cases. When it comes to the declaration medium, a distinction must be made as to whether the text is physically available in its original form and, in addition, is stored on an electronic medium, or whether it is not physically available, i.e. purely digital.²⁸ In the case of transmission, a distinction must be made between physical transmission of the declaration medium (e.g. mailing of paper, USB stick, etc.) and purely virtual transmission.

[70] If the content of the declaration is physically available, then the physical object is also the declaration medium; in this case, the object is classified as a deed in the classical sense. If the deed is digitized and stored on an electronic storage medium, the digitized version is to be regarded merely as a copy of the deed.

[71] If the declaration content is stored as text in a non-physical form, e.g. as a PDF in a cloud, on a USB stick or as text on a mail server, it must be ensured that the corresponding storage format is durable and permanent, and that the text is stored in such a way that it is resistant to change and can be physically reproduced. The Swiss Federal Supreme Court has ruled that an electronically stored PDF document satisfies the criteria of permanence and durability (BGE 9C_597/2014 of December 10, 2014 deliberation 4.5). In the case of electronic storage media, the requirement of physical reproducibility is met if the electronic storage medium allows for the medium content to be reproduced. Proof of document integrity (i.e. that it has not been subsequently altered) is ensured by the electronic signature (see chapter 5.1.3 below).

[72] When transmitting the content of the declaration, the focus must be on whether it can be done in such a way that the integrity and authenticity of the content can be ensured. This will also have to be ensured by the electronic signature.

[73] Therefore, the type of declaration medium is basically irrelevant, provided that a visually perceptible text can be stored in permanent, physically reproducible, and change-resistant form.

²⁸ Cf. GISLER (1999), 128 pp., who distinguishes between «electronic» (= virtual, digital) and «digital» (= digitized, originally paper-based) documents.

In the case of electronic transmission, the criterion of text integrity, i.e. change resistance, is of central importance.

[74] From today's perspective, the criterion of physical reproducibility must be fundamentally questioned. Although physicality bears a certain security relevance, its significance is outdated. Even purely digital data can now be protected in such a way that it is safe from manipulation.

b. Smart Contract as Declaration Medium

[75] As already explained, a contract can either be concluded outside the smart contract and deposited as a hash value on the blockchain or it can be set up directly by means of a smart contract. If the contract is concluded outside the smart contract, then the question of the declaration medium is assessed according to what has been agreed there. If the basic transaction concluded outside the smart contract is stored as a hash value on the blockchain, then the blockchain still serves to verify the integrity of the document. In combination with a hash value stored on the blockchain, the integrity of a document can be determined without the declaration medium having to be assigned special change-resistant properties for this purpose. However, it should be noted that no document can be produced from a hash value; a hash value, conversely, can be derived from a document. It can therefore be determined whether the document has been modified, but not how.

[76] If we assume that the smart contract itself represents the contract, then it also represents the declaration medium. In this case, from a technological perspective, at least the criterion of durability and permanence is met if the smart contract itself is stored on the blockchain. Nevertheless, the criterion of permanence must be questioned in this context, since the continued existence of the blockchain is only granted as long as the P2P participants are willing to maintain the network. This is difficult to assess from today's perspective and must be seen with a certain degree of skepticism due to the (relative) novelty of the technology. If the smart contract is stored in a virtual container, its durability and permanence cannot be affirmed.

[77] Physical reproducibility would also have to be ensured (technically) if a smart contract had to be qualified. A smart contract can therefore only be considered as a suitable means of declaration if, firstly, it represents the contract itself, secondly, it is stored directly on a blockchain, thirdly, the blockchain has a certain stability and, fourthly, the physical reproducibility of the content of the declaration (*in casu* the programming) can be guaranteed. In summary, it can therefore be noted that, from today's perspective, a smart contract is generally not suitable as a declaration medium.

5.1.3. Signature

[78] In Swiss law, the key element of simple written form is the contracting parties' signature. With their signature, the parties acknowledge the content of the contract and express their intention to conclude it. Swiss law has placed the qualified electronic signature on an equal footing with the handwritten signature – the signature can therefore be placed either by hand or by means of a qualified electronic signature under the content of the declaration.

a. Signature in e-Commerce Transactions

[79] In e-commerce transactions, the use of the qualified electronic signature is a plausible option. The qualified electronic signature has had the same status as a handwritten signature since 2005; nonetheless, it has not become the gold standard in (Swiss) commercial transactions. This may be due to the lack of user-friendliness often cited or the lack of interest on the part of the general public (cf. WEBER 2010, 322).²⁹ The qualified electronic signature can prove the identity of the signatory of the message, the authenticity of a document as well as its integrity (GAUCH et al. 2020, n 519b; WEBER 2010, 325; Swiss Federal Council 2014, 1001, 1016).

b. Signature with Smart Contracts

[80] Generally, electronic signatures are used to make transactions on all blockchain platforms and blockchain applications. Consequently, asset transfers via smart contracts also occur through signed transactions.³⁰ As of today, however, no signature keys are used on the known blockchain networks that have been recognized as qualified electronic signatures by the competent certification authority in Switzerland – regardless of whether they would meet the requirements or not. In other words, the (currently) globally used electronic signatures on blockchains are not sufficient to meet the Swiss requirement of simple written form. In order to meet the formal requirement of simple written form nevertheless, a blockchain application provider would have to resort to already recognized qualified electronic signatures or seek recognition accordingly.³¹

5.1.4. Preliminary Conclusion

[81] In summary, it can be noted that a smart contract does not satisfy the requirement of simple written form under Swiss law.³²

5.2. Qualified Written Form

[82] Qualified written form presupposes an additional requirement compared to simple written form, which can be either substantive or formal (BERGER 2018, n 763; GAUCH et al. 2020, n 521; SCHWENZER 2016, n 31.16). The nature of the additional requirement depends on the respective legal provision. For example, for testamentary dispositions, personal handwriting is required (art. 505 CC), or for the termination of rental and business premises, the use of a specific form is mandatory (art. 266l CO). Insofar as the additional requirement for qualified written form is of a substantive nature, it must be reflected in the contract. If the requirements are of a formal nature, it must be checked whether they can also be reproduced digitally. For example, the requirement

²⁹ The requirements for qualified electronic signatures are governed by the Federal Act on Certification Services in the Field of Electronic Signatures and Other Applications of Digital Certificates of March 18, 2016, SR 943.03.

³⁰ It should be noted that a smart contract implemented directly on the blockchain does not have its own private key; the transaction is validated by all nodes.

³¹ The US state of Arizona has acted more progressively. In the House Bill 2417, not only was the term smart contract defined, but regulation was also established that blockchain signatures should be considered valid electronic signatures under the applicable law (in detail and with further references SVIKHART, 2017; cf. BAL 2019, 15).

³² According to TRILLMICH et al. (2020, 179), however, a smart contract satisfies the textual form stipulated in German law. Regarding regulatory need for action under Swiss Law cf. WEBER 2019, 200 and 2018 1, 295.

of personal handwriting can never be met by a purely digital text. In the case of forms required by the Swiss cantons for tenancy law matters, e.g. for the termination of rental and business premises, it has to be considered whether the cantonal law permits digital forms. If the additional requirement can be represented digitally and is permitted by law, then qualified written form could also find its way into e-commerce and smart contracts (provided that electronic signatures used are recognized in the future). This is most likely to be the case with formal requirements such as the obligation to use a form, which could easily be transferred to the digital sphere. Under the current circumstances of Swiss law, however, smart contracts do not meet the formal requirement of qualified written form.

5.3. Public Certification

[83] In public certification, a legally relevant fact or declaration is recorded by a notary (BERGER 2018, n 764; GAUCH et al. 2020, n 524; SCHWENZER 2020, n 31.16). In Switzerland, the form of public notarization is not regulated at federal, but at cantonal level (art. 55a final title CC). Since the complete revision of the Regulation on the Creation of Electronic Public Deeds and Electronic Authentications (EÖBV), which has been in force since February 1, 2018, electronic public deeds and electronic authentications are deemed as equivalent to the corresponding documents in paper form (art. 3 EÖBV, art. 55o final title CC). The legal basis for electronic public authentication has thus been created. Whether blockchain technology will be used in this process in the foreseeable future remains to be seen due to the high level of legal certainty provided by the existing systems in Switzerland. In any event, smart contracts do not currently meet the requirements for public certification form in Switzerland.

5.4. Consequences of Formal Invalidity

[84] Violation of any of the aforementioned formal requirements shall render the contract null and void. Under certain circumstances, however, the contract may be converted into a valid transaction or, for that matter, reversed. The formal requirements and the legal consequences resulting from a breach thereof apply to all legal transactions, regardless of whether they are concluded physically or virtually.

5.4.1. Nullity and Partial Nullity

[85] In Swiss law, a formal requirement is considered to be a validity requirement. According to the Swiss Federal Supreme Court, the violation of a formal requirement causes the nullity of the contract; any person can invoke this circumstance that must be observed *ex officio* (BGE 112 II 330 deliberation 2b p. 334 p, 106 II 146 deliberation 3 p. 151; BERGER 2018, n 771; GAUCH et al. 2020, n 549; SCHWENZER 2020, n 31.27). However, the Federal Supreme Court qualifies the absolute nullity by applying the abuse of a right principle (art. 2 CC; BGE 138 III 40 deliberation 2.3.1 p. 404; BERGER 2018, n 772). Whether there is abuse of a right is to be assessed on a case-by-case basis. The Federal Supreme Court has affirmed abuse of rights, for example, in the case of mutual fulfillment of formally invalid contracts, in the case of fraudulent induction of formal defect or in the case of conscious acceptance of formal defect and formal invalidity asserted thereupon (cf. BGE 138 III 401 deliberation 2.3.2 p. p. 4.4; further lists and references in GAUCH et al.

2020, n 554; SCHWENZER 2020, n 31.31 pp.). The prevailing doctrine advocates a differentiated approach and does not assume absolute nullity, but rather relative nullity or nullity *sui generis*, which can be remedied and only asserted by the parties themselves (BUCHER, OR AT, 169; BERGER, Allgemeines Schuldrecht, n 773; GAUCH et al. 2020, N 561; in detail and with further references SCHWENZER/FOUNTOULAKIS 2020, art. 11 n 23 pp.). If the formal defect is culpably caused by one party and the other party successfully invokes this formal defect, it may additionally be liable for damages based on *culpa in contrahendo* (GAUCH et al. 2020, n 583; SCHWENZER 2020, n 31.42).

[86] Regarding the nullity (or partially nullity) of a smart contract, reference can be made to what has been discussed above in chapter 2.2; the invalidity of a smart contract or a transaction cannot be recorded on a blockchain.

5.4.2. Reversal and Conversion

[87] As explained in the introduction (chapter 5.4), depending on the circumstances, an invalid transaction can be reinterpreted as a valid one (conversion) or, where this is not possible and where no abuse of rights can be observed, it can be reversed (cf. GAUCH et al. 2020, n 584b; SCHWENZER/FOUNTOULAKIS 2020, art. 11 n 25 pp.). In principle, a smart contract cannot be technically unwound. However, a new transaction can be carried out, which in effect reverses the result of a smart contract by means of a new transaction. From a technical point of view, a conversion does not seem to be problematic, since the result of the smart contract keeps its validity.

5.5. Conclusion

[88] Smart contracts do not meet the formal requirements of simple or qualified written form and public certification. In the near future, the requirement of simple written form could be considered as met where qualified persons use legally compliant (qualified electronic) signatures and where the subject of an agreement does not affect any third-party interests.

[89] The violation of formal requirements induces nullity or partial nullity of a contract, depending on the doctrine followed. If a smart contract violates a formal requirement, then the contract's voidness cannot be reflected on a blockchain platform, as no transactions can be subsequently altered or invalidated. However, a *de facto* reversal in the form of a new transaction or a conversion is possible.

6. Summary and Outlook

[90] Due to the freedom of form of Swiss contract law, it is generally possible to draft a contract in programming language.

[91] If a smart contract is used by qualified persons able to understand its content, the smart contract may itself constitute the contract – in the form of a conditional contract. If, on the other hand, it is used by persons unfamiliar with the subject matter, it must be assumed that the persons are not aware of the consequences of what has been agreed, i.e. their intention to be legally bound is not aligned with the possible consequences of the use of a smart contract. In such cases, however, if the parties are consciously unaware of what has been agreed, invoking the lack of the intention to be legally bound can be considered abuse of rights at best. If a smart contract

is concluded by a qualified person and an unqualified person, the situation needs to be assessed on a case-by-case basis. In principle, however, it can be affirmed that in cases where the content of the smart contract is understandable with reasonable effort and the unqualified person is not a consumer, the smart contract can also directly represent the underlying transaction.

[92] As in the case of a computer declaration, the executed smart contract actions can always be assigned to at least one party, since on the one hand an asset is transferred to the smart contract and from there to another (or back to the same) party. Through these transaction(s), the persons involved in a smart contract can be determined and thus all actions of the smart contract can be assigned to these parties.

[93] A smart contract, when placed directly on a public blockchain, cannot be deleted, revoked or modified. A transaction made on the blockchain based on a void underlying transaction cannot be marked accordingly. This leads to some legal uncertainty regarding the validity of blockchain-based transactions and contradicts the principle of blockchain logic, according to which transactions stored on the blockchain are to be considered valid according to the agreed consensus. The same applies to smart contracts that are stored outside a blockchain and whose result (the transaction) was already recorded in the blockchain before the underlying transaction was declared void.

[94] The formal requirements of simple and qualified written form and public certification cannot be met by smart contracts. The requirement of simple written form could in theory be satisfied by the use of certified compliant signatures. However, it appears that such signatures are not in use in any blockchain and even if they were used for smart contracts, it should be noted that the corresponding transaction would bear the signature of the person obligated to sign – smart contracts do not have provide their own signature. Having said that, even a signature assigned to a smart contract would not meet the requirement of written form due to the lack of legal personality. In addition, the signed declaration content would have to be accessible to the parties in writing and language, and, if a third party were affected (e.g., in the case of an assignment of claims), it would have to be accessible to the general public. Programming language is only accessible to qualified persons and not to the general public; the agreement would therefore only be deemed effective when concluded between qualified persons.

[95] Although some hurdles must still be overcome in (Swiss) private law before smart contracts are widely used as «real» contracts with sufficient legal certainty, this situation might change in the foreseeable future. The digitalization of business and private life is advancing rapidly and inexorably, which cannot be ignored by legal practice and doctrine. Well-established concepts and principles, e.g. requirements for the valid conclusion of contracts, can be transferred into the digital world, whereby its specificities must be taken into full account, particularly when it comes to formal requirements.

7. References

ANTONOPOULOS, ANDREAS M. (2015): *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Sebastopol: O'Reilly UK Ltd.

BACON, LEE & BAZINAS, GEORGE (2017): «Smart Contracts»: The Next Big Battleground? In: Jusletter IT May 18, 2017.

- BAL, ALEKSANDRA (2019): Taxation, virtual currency and blockchain. Alphen aan den Rijn, The Netherlands: Wolters Kluwer.
- BALSCHWEIT, PHILIPP (2005): Konsumvertragsrecht und E-Commerce. Bern: Stämpfli Verlag AG.
- BERGER, BERNHARD (2018): Allgemeines Schuldrecht. Schweizerisches Obligationenrecht Allgemeiner Teil mit Einbezug des Deliktsrechts und Einführung in das Personen- und Sachenrecht. Bern: Stämpfli Verlag AG.
- BUGG, STUART (2020): Contracts in English. An introductory guide to understanding, using and developing «Anglo-American» style contracts. 4th edition. Munich: C.H.Beck.
- BOOG, MARKUS (2019): Art. 110 StGB. In: Marcel Alexander Niggli & Hans Wiprächtiger (Eds.): Basler Kommentar, Strafrecht I, Art. 1–110 StGB und Jugendstrafgesetz. 4th edition. Basel: Helbing Lichtenhahn Verlag.
- BRUMMER, CHRIS (2020): Fintech Law in a nutshell. St.Paul: West Academic Publishing.
- BUCHER, EUGEN (1988): Schweizerisches Obligationenrecht. Allgemeiner Teil ohne Deliktsrecht. 2nd edition. Zurich: Schulthess Verlag.
- CHRISTIDIS, KONSTANTINOS & DEVETSIKIOTIS, MICHAEL (2016): Blockchains and Smart Contracts for the Internet of Things. In: IEEE Access, 2016 (4), p. 2292–2303. <https://ieeexplore.ieee.org/document/7467408>.
- CARRON, BLAISE & BOTTERON, VALENTIN (2019): How smart can a contract be? In: Daniel Kraus, Thierry Obrist & Olivier Hari (Eds.): Blockchains, smart contracts, decentralised autonomous organisations and the law. Cheltenham: Edward Elgar Publishing. P. 101–143.
- COSTANTINI, FEDERICO, FERENCZ, BALINT & NAGYPÁL, SZABOLCS (2021): «Code is Law» and smart contracts. Embedding ethics in decentralized ledger systems. In: Jusletter IT May 27, 2021.
- CLACK, CHRISTOPHER D., BAKSHI, VIKRAM A. & BRAINE, LEE (2016): Smart Contract Templates: Foundations, Design Landscape and Research Directions. <https://arxiv.org/abs/1608.00771>.
- DE FILIPPI, PRIMAVERA & WRIGHT, AARON (2019): Blockchain and the law: the rule of code. First Harvard University Press paperback edition. Cambridge (Massachusetts): Harvard University Press.
- DASSER, FELIX (2021): Art. 358 ZPO. In: Paul Oberhammer, Tanja Domej & Ulrich Haas (Eds.): Kurzkommmentar ZPO, Schweizerische Zivilprozessordnung. 3th edition. Basel: Helbing Lichtenhahn Verlag.
- EGGEN, MIRJAM (2016): Home Smart Home. In: AJP, 2016 (9), P. 1131–1140.
- EGGEN, MIRJAM & SILLABER, CHRISTIAN (2020): DLT-Handelssysteme: eine Einordnung in das Zivil- und Aufsichtsrecht. In: Jusletter May 11, 2020.
- EHRAT, FELIX R. & WIDMER, MARKUS (2019): Vorbemerkungen zu Art. 151–157 OR, Art. 151, 154 OR. In: Corinne Widmer Lüchinger & David Oser (Eds.): Basler Kommentar, Obligationenrecht I, Art. 1–529 OR. 7th edition. Basel: Helbing Lichtenhahn Verlag.
- ELLUL, JOSHUA, GALEA, JONATHAN, GANADO, MAX, MCCARTHY, STEPHEN & PACE, GORDON J. (2020): Regulating Blockchain, DLT and Smart Contracts: a technology regulator’s perspective. ERA-Forum 21 (2), P. 209–220. <https://link.springer.com/article/10.1007/s12027-020-00617-7>.
- EPINEY, ASTRID (2015): Art. 5 BV. In: Bernhard Waldmann, Eva Maria Belser & Astrid Epiney (Eds.): Basler Kommentar, Bundesverfassung. Basel: Helbing Lichtenhahn Verlag.

FANKHAUSER, ROLAND (2018): Art. 11, 12, 16, 17, 18 ZGB. In: Thomas Geiser & Christina Fountoulakis (Eds.): Basler Kommentar, Zivilgesetzbuch I, Art. 1–456 ZGB. 6th edition. Basel: Helbing Lichtenhahn Verlag.

FERENCZ, BÁLINT (2020): Smart contracts: the legal comparison. In: Jusletter IT September 30, 2020.

FINCK, MICHÈLE (2019): Blockchain regulation and governance in Europe. Cambridge: Cambridge University Press.

FURRER, ANDREAS (2018): Die Einbettung von Smart Contracts in das schweizerische Privatrecht. In: Anwaltsrevue, 2018 (3), p. 103–115.

GAUCH, PETER, SCHLUEP, WALTER R., SCHMID, JÖRG & EMMENEGGER, SUSAN (2020): Schweizerisches Obligationenrecht Allgemeiner Teil, ohne ausservertragliches Haftpflichtrecht, 2 volumes. 11th edition. Zurich: Schulthess Verlag.

GIRSBERGER, DANIEL (2017): Art. 358 ZPO. In: Karl Spühler, Luca Tenchio & Dominik Infanger (Eds.): Basler Kommentar, Schweizerische Zivilprozessordnung (ZPO). 3th edition. Basel: Helbing Lichtenhahn Verlag.

GIRSBERGER, DANIEL & HERRMANN, JOHANNES L. (2019): Art. 164 OR. In: Corinne Widmer Lüchinger & David Oser (Eds.): Basler Kommentar, Obligationenrecht I, Art. 1–529 OR. 7th edition. Basel: Helbing Lichtenhahn Verlag.

GISLER, MICHAEL (1999): Vertragsrechtliche Aspekte Elektronischer Märkte: nach Schweizerischem Obligationenrecht. St. Gallen: University of St.Gallen (Dissertation).

GRÄNICHER, DIETER (2021): Art. 178 IPRG. In: Pascal Grolimund, Leander D. Loacker & Anton K. Schnyder (Eds.): Basler Kommentar, Internationales Privatrecht. 4th edition. Basel: Helbing Lichtenhahn Verlag.

GRIGG, IAN (2000): Financial Cryptography in 7 Layers, 4th Conference on Financial Cryptography. Anguilla: Springer-Verlag LNCS 1962. P. 332–348.

GRÜNEWALD, SERAINA (2015): Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen. In: Rolf H. WEBER & Florent Thouvenin (Eds.): Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme. Zurich: Schulthess Verlag. P. 93–112.

GUILLAUME, FLORENCE (2019): Aspects of private international law related to blockchain transactions. In: Daniel Kraus, Thierry Obrist & Olivier Hari (Eds.): Blockchains, smart contracts, decentralised autonomous organisations and the law. Cheltenham: Edward Elgar Publishing. P. 49–82.

GYR, ELEONOR (2017): Dezentrale Autonome Organisation DAO. In: Jusletter December 4, 2017.

- (2019): Blockchain und Smart Contracts. Die vertragsrechtlichen Implikationen einer neuen Technologie. Bern: University of Bern (Dissertation).
https://biblio.unibe.ch/download/eldiss/19gyr_e.pdf.

HAAPIO, HELENA (2020): Transforming Contract Creation: Goodbye to Legal Writing – revisited. In: Jusletter IT September 30, 2020.

HAUSHEER, HEINZ & AEBI-MÜLLER, REGINA E. (2012): Art. 2 ZGB. In: Heinz Hausheer & Hans Peter Walter (Eds.): Berner Kommentar, Einleitung, Art. 1–9 ZGB Schweizerisches Zivilgesetzbuch, Einleitung und Personenrecht. Bern: Stämpfli Verlag AG.

- HEROLD, HELMUT, LURZ, BRUNO, WOHLRAB, JÜRGEN & HOPF, MATTHIAS (2017): Grundlagen der Informatik. 3th edition. Hallbergmoos: Pearson Studium.
- HOEREN, THOMAS (2018): Internetrecht, ein Grundriss. 3th edition. Berlin/Boston: De Gruyter.
- HOFER SIBYLLE & HRUBESCH-MILLAUER, STEPHANIE (2012): Einleitungsartikel und Personenrecht. 2nd edition. Bern: Stämpfli Verlag AG.
- HONSELL, HEINRICH (2018): Art. 2 ZGB. In: Thomas Geiser & Christina Fountoulakis (Eds.): Basler Kommentar, Zivilgesetzbuch I, Art. 1–456 ZGB. 6th edition. Basel: Helbing Lichtenhahn Verlag.
- HUGUENIN, CLAIRE (2011): Zum Verhältnis zwischen linguistischen Kommunikationsmodellen und Verträgen. In: Rolf Sethe et al. (Eds.): Kommunikation, Festschrift für Rolf H. Weber zum 60. Geburtstag. Bern: Stämpfli Verlag AG. P. 109–121. https://www.zora.uzh.ch/id/eprint/51671/1/Huguenin_Kommunikation_FS_Weber_2011.pdf.
- HUGUENIN, CLAIRE (2019): Obligationenrecht. Allgemeiner und Besonderer Teil. 3th edition. Zurich: Schulthess Verlag.
- HUGUENIN, CLAIRE & MEISE, BARBARA (2019): Art. 19/20 OR. In: Corinne Widmer Lüchinger & David Oser (Eds.): Basler Kommentar, Obligationenrecht I, Art. 1–529 OR. 7th edition. Basel: Helbing Lichtenhahn Verlag.
- HÜRLIMANN-KAUP, BETTINA (1999): Die privatrechtliche Gefälligkeit und ihre Rechtsfolgen. Freiburg i.Ü.: University press.
- HÜRLIMANN-KAUP, BETTINA & SCHMID, JÖRG (2016): Einleitungsartikel des ZGB und Personenrecht. 3th edition. Zürich: Schulthess Verlag.
- ISLER, MICHAEL (2017): Datenschutz auf der Blockchain. In: Jusletter December 4, 2017.
- KAULARTZ, MARKUS (2016): Die Blockchain Technologie: Hintergründe zur Distributed Ledger Technologie und zu Blockchains. In: CR. 2016 (7), p. 474–480.
- KAULARTZ, MARKUS & HECKMANN, JÖRN (2016): Smart Contracts: Anwendung der Blockchain Technologie. In: CR. 2016 (9), p. 618–624.
- KIANICKA, MICHAEL MARTIN (2012): Die Agentenerklärung. Elektronische Willenserklärungen und künstliche Intelligenz als Anwendungsfall der Rechtsscheinhaftung. Zurich: Schulthess Verlag.
- KLASS, GREGORY (2010): Contract Law in the USA. Alphen aan den Rijn: Wolters Kluwer.
- KRAMER, ERNST A. (1991): Berner Kommentar, Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, Allgemeine Bestimmungen: Der Inhalt des Vertrages, Art. 19–22 OR. Bern: Stämpfli Verlag AG.
- KRAMER, ERNST A. & SCHMIDLIN, BRUNO (1986): Berner Kommentar, Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, Allgemeine Bestimmungen: Die Entstehung durch Vertrag, Art. 1–18 OR. Bern: Stämpfli Verlag AG.
- KRAMER, ERNST A., PROBST, THOMAS & PERRIG, ROMAN (2016): Schweizerisches Recht der Allgemeinen Geschäftsbedingungen. Bern: Stämpfli Verlag AG.
- KRYPZCYK, VEIKKO & BOCHKOR, OLENA (2015): Programmieren für Einsteiger: Teil 1. Frankfurt a.M.: entwickler.press.
- MAUME, PHILIPP, MAUTE, LENA & FROMBERGER, MATHIAS (2020): Rechtshandbuch Kryptowerte: Blockchain, Tokenisierung, Initial Coin Offerings. Munich: C.H.Beck.

- MEYER, STEPHAN D. & SCHUPPLI, BENEDIKT (2017): Smart Contracts und deren Einordnung in das schweizerische Vertragsrecht. In: recht 2017, p. 204–224.
- MIELKE, BETTINA & WOLFF, CHRISTINA (2018): «Klar ist der Aether und doch von unergründlicher Tiefe»: Smart Contracts als interdisziplinäres Problem. In: Jusletter IT February 22, 2018.
- MIK, ELIZA (2017): Smart Contracts: Terminology, Technical Limitations and Real World Complexity. In: Law, Innovation and Technology, 9(2)/2017, p. 269–300.
- MOUGAYAR, WILLIAM (2016): The Business Blockchain. Promise, Practice, and Application of the Next Internet Technology. Hoboken: John Wiley & Sons Inc.
- PEEL, EDWIN (2020): The Law of Contract, 15th edition. London: Thomson Reuters.
- PLOOM, TARMO (2016): Blockchains: wichtige Fragen aus IT-Sicht. In: Daniel Burgwinkel (Ed.): Blockchain Technology, Einführung für Business und IT-Manager. Berlin/Boston: De Gruyter. P. 123–148.
- REDEKER, HELMUT (2020): IT-Recht. 7th edition. Munich: C.H. Beck.
- RICHTER, THOMAS (2020): Blockchain Regulation. In: Matthias Artzt & Thomas Richter (Eds.): Handbook of blockchain law: a guide to understanding and resolving the legal challenges of blockchain technology. Alphen aan den Rijn: Wolters Kluwer. P. 123–161.
- ROWLAND, DIANA, KOHL, UTA & CHARLESWORTH, ANDREW (2016): Information Technology Law. 5th edition. Abingdon/New York: Routledge.
- SCHALLER, JEAN-MARC (2018): Blockchain Serie, blogpost 32 (FinBlog, <https://www.finblog.ch/>).
- SCHÄR, FABIAN & BERENTSEN, ALEKSANDER (2020): Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction. Cambridge & London: The MIT Press.
- SCHMID, JÜRIG (2019): Art. 975 ZGB. In: Thomas Geiser & Stephan Wolf (Eds.): Basler Kommentar, Zivilgesetzbuch II, Art. 457–977 ZGB und Art. 1–61 SchlT ZGB. 6th edition. Basel: Helbing Lichtenhahn Verlag.
- SCHMIDLIN, BRUNO (2013): Berner Kommentar, Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, Allgemeine Bestimmungen, Mängel des Vertragsabschlusses, Art. 23–31 OR. 2th edition. Bern: Stämpfli Verlag AG.
- SCHWENZER, INGEBORG & FOUNTOLAKIS, CHRISTINA (2020): Art. 11, 13 OR. In: Corinne Widmer Lüchinger & David Oser (Eds.): Basler Kommentar, Obligationenrecht I, Art. 1–529 OR. 7th edition. Basel: Helbing Lichtenhahn Verlag.
- SCHWENZER, INGEBORG (2020): Schweizerisches Obligationenrecht Allgemeiner Teil. 8th edition. Bern: Stämpfli Verlag AG.
- SHIER, CHARLES, MEHAR, MUHAMMAD, IZAHAR, GIAMBATTISTA ALANA, GONG, ELGAR, SANAHYIE, RYAN, KIM, HENRY & LASKOWSKI, MAREK (2017): Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack. In: SSRN 3014782, 2017. <https://ssrn.com/abstract=3014782>.
- SIXT, ELFRIEDE (2017): Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie. Wiesbaden: Gabler Verlag.
- STEINAUER, PAUL-HENRI & FOUNTOLAKIS, CHRISTIANA (2014): Droit des personnes physiques et de la protection de l'adulte. Bern: Stämpfli Verlag AG.
- SVIKHART, RILEY T. (2017): Blockchain's Big Hurdle. Stanford Law Review. <https://review.law.stanford.edu/wp-content/uploads/sites/3/2017/11/70-Stan.-L.-Rev.-Online-100-Svikhart.pdf>.

Swiss Federal Council (2014): Botschaft zur Totalrevision des Bundesgesetzes über die elektronische Signatur (ZertES) of January 15, 2014, BBl 2014, p. 1001–1038. <https://www.fedlex.admin.ch/eli/fga/2014/171/de>.

- (2014): Bericht zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) of June 25, 2014. <https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf>.

SZABO, NICK (1994): Smart Contracts. www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

- (1997): The Idea of Smart Contracts. www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

TAPSCOTT, DON & TAPSCOTT, ALEX (2016): Blockchain Revolution. How the Technology Behind Bitcoin is Changing Money, Business, and the World. New York: Random House N.Y.

TIMMERMANN, DANIEL (2020): Legal Tech-Anwendungen. Rechtswissenschaftliche Analyse und Entwicklung des Begriffs der algorithmischen Rechtsdienstleistung. Baden-Baden: Nomos.

TRILLMICH, PHILIP, GOETZ, MATTHIAS & EWING, CHRIS (2020): Blockchain and Smart Contracts. In: Matthias Artzt & Thomas Richter (Eds.): Handbook of blockchain law: a guide to understanding and resolving the legal challenges of blockchain technology. Alphen aan den Rijn: Wolter Kluwers. P. 163–192.

WEBER, ROLF H. (2002): Freie Software – Befreiung vom Vertragstypenkonzept? In: Friedrich Harrer, Wolfgang Portmann & Roger Zäch (Eds.): Besonderes Vertragsrecht – aktuelle Probleme. Festschrift für Heinrich Honsell zum 60. Geburtstag. Zurich: Schulthess. P. 41–57.

- (2010): E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen. 2th edition. Zurich: Schulthess Verlag.
- (2017): Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts. In: Jusletter December 4, 2017.
- (2018 1): Smart Contracts: Vertrags- und verfügungsrechtlicher Regelungsbedarf. In: sic! 2018, issue 6. P. 291–301.
- (2018 2): «Rose is a rose is a rose is a rose» – what about code and law? In: Computer Law and Security Review. P. 701–706.
- (2019): Smart Contracts: Do we need New Legal Rules? In: Alberto De Franceschi & Reiner Schulze (Eds.): Digital revolution – new challenges for law: data protection, artificial intelligence, smart products, blockchain technology and virtual currencies. Baden-Baden: Nomos/München: C.H.Beck. P. 299–312.
- (2020): Linguistische Kommunikation und technischer Code in Verträgen. In: Gedenkschrift für Claire Huguenin. Zurich: Dike. P. 495–505.

WEBER, ROLF H. & JÖHRI, YVONNE (2000): Vertragsabschluss im Internet. In: Rolf H. Weber, Reto M. Hilty & Rolf Auf der Maur (Eds.): Geschäftsplattform Internet. Rechtliche und praktische Aspekte. Zurich: Schulthess Verlag. P. 39–57.

WEBER, ROLF H. & WEBER, ROMANA (2010): Internet of Things. Legal Perspectives. Zurich: Schulthess Verlag.

XOUDIS, JULIA (2012): Art. 13 OR, In: Luc Thévenoz & Franz Werro (Eds.): Commentaire Romand, Code des obligations I, Art. 1–529 CO. 2nd edition. Basel: Helbing Lichtenhahn Verlag.

ZELLWEGGER-GUTKNECHT, CORINNE & BUCHER, EUGEN (2019): Art. 1 OR. In: Corinne Widmer Lühinger & David Oser (Eds.): Basler Kommentar, Obligationenrecht I, Art. 1–529 OR. 7th edition. Basel: Helbing Lichtenhahn Verlag.

ZIMMERMANN, REINHARD & WHITTAKER, SIMON (2000): Good faith in European contract law. Cambridge: Cambridge University Press.

Dr. iur. ELEONOR GYR is Attorney-at-law at Gyr Gössi Olano Staehelin in Basel.

Many thanks to MLaw Eleonora Heim for her valuable support in the research.