BLOCKCHAIN COMPLIANCE

Peter Ebenhoch

Dr., PMP, Senior Consultant, effectas GmbH
Bundesstrasse 6, 6300 Zug, CH
peter.ebenhoch@effectas.com; http://www.lean-grc.com

Keywords: ***Blockchain, Governance, Risk, Compliance, Standardization, FinTech, RegTech***

Abstract: *This article explores options to embed blockchains and their applications in the legal context de lege lata and de lege ferenda. Blockchains introduce analog scarcity into digital abundance. Beyond the sucess of Bitcoins as digital currency, they promise new options to organize institutions, to manage public ledgers and to setup and complete deals with so-called «smart contracts». At the end of the day, the «blocks» are simply digital objects in an IT system and many established legal concepts can be applied problem-free. However, to create valid legal effects blockchains should be anchored prudently in the surrounding legal context and specific regulations will be supportive to unfold their potential in a sustainable way and in an international context.*

1. The Challenge

Legal compliance and regulation activities as well as technical standardization attempts are delayed by nature: Regularly technical inventions come first and the legal system has to catch up subsequently.

The promises of the blockchain concept, however, threat to undermine established legal functions in essence: Blockchain currencies, land registers, electricity auctions, so-called ICOs (Initial Coin Offerings) and even the generic formation of contracts, provided with «Smart Contracts» and housed by blockchains, seem to establish a shadow legal system in its own right and at a very fast pace, without waiting for formal acknowledgment by established «analog» law.

Despite being in the public eye, reflections about the legal anchoring and appropriate regulatory concepts are quite rare. This article aims to remedy this situation by trying to answer the following questions:

How can we pave the way to utilize the potential of blockchains in a legal viable way and avoid general prohibitions as imposed recently by China, which even included a retrospective ban[1]*?*

2. Critical Success Factors

So far, only states have had the formal power to enact laws and to execute them. And nearly each state has made extensive use of this legislation power. That said, it is clear that *de lege lata* each blockchain activity takes place in a binding legal context, no matter how good or bad the rules fit.

However, in case the rules are way off, they become ineffective. Therefore, it is also clear that there are good reasons to align regulation with new technical concepts and implementations *de lege ferenda*. In our globalized society and in particular when dealing with agile IT startups, we have to be aware that each subject to the law can stay in conformity simply by moving to another legislation area. And when dealing with blockchains even those who ignore strict prohibitions cannot easily be pursued because of the integrally decentralized and resilient character of the technology.

[1] Kleinz 2017, with reference to: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html (all websites last visited on 30 January 2018).

The starting point of the discussion will be the Etherum «The DAO hack» and the questions it raised in relation to the existing legal context. Then I will touch on what can be done to embed blockchain applications in the existing legal context[2]. Subsequently, I will discuss what is needed *de lege ferenda* to create regulations to best utilize the potential of blockchains[3].

3. Preliminary Remark: Compliance and Regulatory Efforts as a Myth of Sisyphos?

It is a modern fairy tale that disruptive and innovative technologies come first, driven by powerful, wealthy and lofty tech giants serving the well-being of mankind, and that legal compliance follows after, conducted by underfunded and bureaucratic people, often in analog dumbness, threatening the digital progress at stake. We are also told that blockchain regulation is actually missing, causing unsteady conditions and erratic case-to-case measures by authorities.

In my opinion, both of these assumptions are wrong: Each technical innovation is created in a society where certain rules and conditions are already in place. This means that the legal context comes first. And each technical innovation removes previously existing restrictions and creates, by doing so, new risk factors, thus asking for new context rules.

Without such context rules, without an appropriate regulation, inventions cannot unfold their full benefit and potential and investments might become misguided. What might lack, therefore, is the focus and energy of a society to supply and catch up with appropriate regulations to make the technical innovation work at its best, to «fill the compliance gap».

4. Blockchain Compliance de lege lata

4.1. Blockchains and its Applications as Humble Distributed Databases

From a legal perspective most discussions about the disruptive and innovative character of blockchain can be mapped to existing, trivial legal use cases and well established legal rules and concepts:

- Many blockchain applications are in effect nothing else than distributed utilizations of excel spreadsheets put on a cloud server, allowing for document versioning and decentralized access[4].
- Even many ICOs/ITOs (initial coin or token offerings respectively) are in essence nothing else than well-known customer retention programs, like collecting frequent flier miles or payback points. Remaining discussions about whether or not to add valued-added tax can be settled easily.
- If one takes money or crypto equivalents for a vague idea without any prospect to roughly realize the propagated expectations, he simply is a fraud because he has deceived someone and damaged others with intention.
- If blockchain applications or concepts fail with regard to poor software quality and program errors, there should be compensation for damages due to a lack of quality of supply.

That said, lawyers and courts are well advised to nobly ignore the buzzword «blockchain», circumvent it for the time being with «distributed excel sheets» or «distributed database» at first and to check how well-known legal concepts and established regulations might be appropriate to solve the case at hand, either by directly applying them or through conclusion by analogy.

However, the soft voice of legal reason is often unheard today and the word «blockchain» seems to have an ecstatic and hypnotic effect.

---

2 In the article «Smart Contexts for Smart Contracts», presented at the IRIS 2018 conference, I examine with Gantner in detail how so-called «smart contracts» can be legally programmed and embedded in a legally compliant way (Ebenhoch/Gantner 2018).

3 Due to space constraints, the question how blockchains can be utilized to provide compliance mechanisms on their own (RegTech for «Regulatory Tech») and for surveillance purposes cannot be discussed here.

4 The original phrase, how Tracy Alloway put it: Alloway 2017.

One reason might be that each blockchain utilization is, in essence, a very sophisticated implementation of encrypted and distributed software engineering. It is so complex that it seems that even its creators do not have enough insight into what they have released to the world.

4.2. The Spectacular Failure of the DAO

4.2.1. Case Description[5]

One prominent example of the hybrids of blockchain developers is «The DAO», which abbreviates «Decentralized Autonomous Organization». It was developed by the German start-up slock.it as an application of the Etherum blockchain. The promise was to setup a new and better way of business organization using smart contracts and realizing «unstoppable code». In the end, it became an unstoppable disaster of programming errors and shortcomings, resulting in an unauthorized withdrawal of at least $50 million.

After it had received $150 million of funding – representing 14% of all Ether[6] available at that time – and ignoring warnings of researchers, a hacker obtained $50 million by simply calling a balance function *recursively*. As the underlying smart contract programming language «Solidity» is intentionally fully Turing complete, this did not seem to be a bug of the underlying Etherum infrastructure and its programming language but simply a mistake of The DAO implementers. However, due to the consensus mechanisms involved it took two weeks to correct the bug by changing the «smart» contract; there was no other way to correct the «unauthorized» withdrawal.

Subsequent discussions reflected whether the withdrawal was even «unauthorized» or whether it was a «hack» at all, because the system was exactly used as it was intended to be used from a technical point of view. The Etherum foundation finally decided on a hard fork, to wind back Etherum and to leave the failed version back as «Etherum classic».

The «steadfast iron will of unstoppable code» had turned out to be a «changeable modelling material of human opportunistic will»; the slogan «code is law» was valid only so long until a bug was found. The request to the hacker to give back the money which was taken in alignment with their mechanism proves the sentimental inability of the persons involved.

4.2.2. Legal Findings

The DAO hack reveals a bunch of legal issues which could be subjects of regulation, obviously also to support the further utilization of blockchains and to prevent such failures in the future and therefore to support blockchain proponents:

- **Accountability** – The DAO as a legal entity: The DAO did not have a formal legal anchorage, so the question came up, as to how it could be treated from a legal perspective. In the end, it has to be regarded as a general partnership or a private corporation with all involved stakeholders (investors, creators, operators) being personally liable.
- **Code is *not* law** – Relationship of code and law: If the stated assumption that Code is Law would have been correct, there would have been no need to wind back the blockchain and to fork Etherum classic. There would have been no incidence at all because everything happened as predefined by the algorithmic and programming context. Obviously, the assumption that code replaces law is simply wrong. The code in place operates always in a legal context which has to be determined and setup appropriately.
- **Error fixation** – missing error correction: The DAO «hack» also revealed a major shortcoming of so-called smart contracts with regard to the option of error correction. Error correction in software development is an expression of learning ability and agility, with regard to creatures it is even a condition

5 Biederbeck 2016.

6 «Ether» is the currency of the Etherum blockchain.

for survival. Blockchains should rely on open source software, so that software errors can be located by a larger audience. Blockchains also should provide mechanisms to fix located errors quickly, though this is obviously in conceptual contradiction to the consensus mechanism.

- **Know Your Customer** – Transparency and identity: Blockchains offer ambiguous transparency. On the one hand every account and its actions are publicly available and fully reproducible, on the other hand the identity of the persons or organizations behind an account are not revealed as it was the case for The DAO «hacker», at least not by the system itself. If one stakeholder reveals the relation of his identity to his account, this can also threaten the anonymity of the other participants. A blockchain creator and operator can also determine his level of identity awareness by requiring full identification before getting access (e.g. via a wallet). If a state operates a blockchain, this will result in full knowledge and power of the state to identify each participant and each transaction without exception.
- **Rollback and liquidation procedures** – Too big to fail: After the financial crisis, discussions on how to avoid banks which are «too big to fail» came up. One idea is to cogently require phaseout procedures covering both legal (phaseout of a legal person) and financial aspects (return deposits). As The DAO case shows, the same principles make sense with regard to blockchains: They should also define rewind and phaseout procedures upfront.
- **Staged ICO** – Uncontrolled offerings: The DAO ICO was, with regard to the plain concept, offered unlimitedly. It raised $150 millions at once. Though it is unclear whether a staged ICO would have changed the course of action, there are good arguments to establish some kind of staged control of ICOs, e.g. with regard to the relationship of business substance (idea – whitepaper – prototype – organization with positive cash flow), to the business model (to sort out Ponzi-scheme like concepts), to the allowed amounts and with regard to the distribution and contribution for individuals and organizational investors.

4.3. Establishing Valid Legal Contexts

4.3.1. State Specific Differences

At the moment, we can notice differing reactions to blockchain regulation in different countries. A few countries like Switzerland and Singapore have been prominent in demonstrating high blockchain acceptance.

- Switzerland has, also with regard to its finance industry, a very strong FinTech and RegTech community and movement, organized around blockchain technology. Particularly well-known are the small city and «Kanton» of Zug, which managed to establish themselves under the brand «crypto valley»[7]. As a resident I can even pay my taxes with Bitcoins and a digital citizen ID based on blockchain technology will become effective in early 2018[8]. However, the Bitcoins are converted each day and the acceptance rate seems to be very modest, so far.
- Singapore's Central Bank's Chief emphasizes to avoid regulation but to be alert about possibly upcoming risks. He does not see the technology risky in itself, but its misuse. At presence, virtual-currency intermediaries such as exchange operators are already regulated with regard to combating money laundering and financing of terrorism[9].
- In Canada adaptive steps are taken to welcome the use of cryptocurrencies and blockchains[10]. The regulators seem to be cautious and intentionally avoiding premature measures.

---

7 «Ehemaliges Schweizer Fischerörtchen Zug als Krypto-Mekka», https://futurezone.at/digital-life/ehemaliges-schweizer-fischeroertchen-zug-als-krypto-mekka/295.150.097, futurezone, 2017. Cf. also https://cryptovalley.swiss/.

8 This is also possible because Swiss «Kantons» have their own legislation and are only partially legally bound by Switzerland as state.

9 Chanjaroen/Tan/Amin 2017.

10 Gourdan 2017.

- So far only China has explicitly forbidden cryptocurrencies. As already mentioned, it sounds reasonable that the highly centralized and authoritarian state wants to avoid decentralized public management developments and will focus on utilizing blockchain for its own centralistic purposes subsequently.
- Due to the fact that internationally aligned regulation is missing, there is a certain competition between states at stake. Each state that prematurely bans blockchain related applications like cryptocurrencies or ICOs will loose interest, talents and money due to its locational disadvantage.
- States like Austria or Germany still have excellent prospects to harvest low hanging fruit and attract the blockchain industry by demonstrating domain specific understanding and appropriate regulation strategies. This seems to be an easy game, however, even that might be asking too much of the currently not established government in Germany and the new right-wing government in Austria. The same seems to be true for the Brexit-focused government in the United Kingdom, who has to hedge its importance as a location for international banking.

4.3.2. General Options

The concept of «private autonomy» means, in essence, that the citizens are empowered to arrange their private legal relationships as they like, within the borders of public law.

As already stated before in 4.1., many so-called legal blockchain challenges can easily be traced back to well-known and acquainted legal issues. However, a critical precondition is a deep understanding of the blockchain concepts and many lawyers might miss these insights and therefore fail to fruitfully apply their knowledge to this new concept. An excess of recommendations and regulations might result of that.

When focusing on the core issues and applying lean principles[11] we can boil the necessary legal framework down to these elements:

1. Legal organization: What kind of organization is planned and makes sense to be utilized? This includes choosing an appropriate legal location.
2. IT organization: What kind of transparency and publicity does the target technology provide and ask for? How are operational aspects reflected and taken into account?
3. Domain specific regulations: Does the venture take place in a specific regulated area, e.g. banking, insurance, etc.?
4. Tax-related issues: Are there probable tax-related issues which can be clarified? If accomplished upfront, this can avoid substantial threats to business models.
5. Stages, stakeholder interests and phaseout: What kinds of stakeholders are involved and what is the legal relationship to each group? Is there a mechanism to start the project and to phase it out in case it fails or faces actual, unforeseen issues?

These five aspects can be clarified with manageable effort upfront and can make sure that the whole project develops with high confidence and integrity.

5. Blockchain Compliance de lege ferenda

5.1. Power Consumption

After the previous exploration of The DAO hack and its implications, it might sound strange to list energy consumption as the first regulatory item. However, high energy consumption is one, if not the greatest, conceptual restriction the current blockchain technology faces. The reason for that is the reliance of the consensus

[11] I have developed a method to focus on legal key issues when dealing with technical compliance, named it «Lean GRC» (abbreviating «*Lean Governance, Risk and Compliance*»). Further information can be found on the dedicated website http://www.lean-grc.com.

mechanism on raw calculation power. The more successful a blockchain based on this concept is, the more miners will be interested and the more calculation power will be needed to grant continuous operation.

Miners already moved to countries with low energy prices. This leads to a high concentration in China, the only country which, ironically, has started to ban cryptocurrencies. At the moment of writing (January 2018) Bitcoins are reported to consume electricity in amounts comparable to the power consumption of a whole country with the size of Bulgaria or Hungary, representing 0.17% of the world energy consumption[12]. Given the reported and already realized changes in our climate, this is more than a minor shortcoming. With regard to this conceptual weakness, blockchain technology was described as the *diesel-technology of IT*.

If energy consumption is restricted and the demand of electricity increases further this can have an effect on the consensus mechanism. It will increase the concentration of miners which is already very high, in particular with regard to Bitcoins[13,14].

5.2. Publicity of Blockchains / Identity Management

Blockchain transactions are fully transparent and visible to all participants, but only with regard to the technical user addresses used within the blockchain. On the one hand, it is initially not revealed which human or legal subject is connected with a technical user account. On the other hand, there is no guarantee that all participants stay anonymous: If a small number of single users reveal their credentials, it can be easily extrapolated by the transactions who the other users are. This is particularly true, when the transactions relate to public ledgers which are connected with identities or real property. In that case, existing partial information and metadata can easily be mixed and checked using Big Data analytics, so that all real blockchain users can be revealed with ease.

If the blockchain is governed by a single operator (e.g. a central bank or a state) it has full control of the identities of the blockchain users anyway. In other cases, this identity management should be the subject of domain specific regulation. With regard to currencies, anti-money laundering (AML) regulations and Know-Your-Customer (KYC) premises can be fully applied.

With regard to public ledgers, KYC as well as the verification and alignment of real assets to the assets stored in the blockchain gets crucial. The blockchain ID of the real estate property has to map 1:1 to the actual real estate property. How the mapping of such blockchain entries to the real world – with its limited analogy resources – is created and managed and who is allowed to map, is not determined by blockchain technology. It has to be determined by the operators of the blockchain[15].

This means that the way access to the blockchain is offered and the trust level of interfaces are also subjects of regulation, depending on the specific domain and its public relevance at stake.

5.3. Transparency and Error Correction

The functionality and routines of blockchains have to be transparent and reproducible. Therefore, a public and decentralized blockchain has to be available as open source code. This also supports the chance to find and fix errors in the underlying source code.

---

12 https://digiconomist.net/bitcoin-energy-consumption.

13 Brodu 2017.

14 It is worth noting that there might be conceptual alternatives to these kinds of power hungry consensus mechanisms and that this restriction actually only applies to blockchains which are completely decentralized and public. An internal blockchain can be run with very modest energy consumption.

15 This is in particular true when blockchains operate in connected mode: If a smart contract exchanges cryptocoins for the ownership of a house for example, there is not only a simple exchange of a certain amount of cryptocoins from one wallet to the other in the same blockchain (e.g. Bitcoin), but also an exchange of cryptocoins and a change of ownership in the land register/ledger, probably in two blockchains which are connected via interfaces. The blockchain technology itself has no unique mechanism to ensure that the real property exists and that the seller is truly that person or legal subject.

5.4. Organizational Accountability

Organizational accountability has to be assured at least with regard to the operation of the blockchain itself.

Though blockchains are described as self-executing and unstoppable, they need IT systems and operation to exist. Given already evident or foreseeable circumstances (e.g. electricity, bugs and security threats, regulation context), there has to be a board/committee in place which takes care of issues. This also implies the task to grant operational qualities like availability and quality of services. And it will clarify questions with regard to compensation for damages due to technical issues or operational mismanagement.

5.5. Regulation of ICOs

As already stated, law is generally more or less prepared to handle the ICO phenomenon. Similar traditional applications like frequent flier miles, customer bonus points etc. are legally settled and therefore traditional rules for IPOs might apply analogously.

Anyhow, given the high interest and large amounts of (real) money involved, it is pretty clear that ICOs should be regulated quickly and best in an internationally aligned effort. At this point, it is very clear that the full application of IPO rules, e.g. the duty to select an investment bank, would limit the potential of ICOs too much. To start with, these three focus points could be clarified:

- Organizational clarity: Who is initiating the ICO? Which legal subjects are entitled to initiate an ICO?
- Legally binding documentation (e.g. white paper) / project state: Content of the ICO? In which state is the project in (e.g. idea, start up, minimum viable product, first customer base, and positive cash flow)?
- Stages as a determination of a certain course of action: Rules about investment cycles with regard to the state the project is in, e.g. rules about participants, investment limits and the spread for each cycle.

The Swiss FINMA (Finance Market Authority) has recently released their assessment of ICOs[16]. They emphasize that they will continue applying existing domain specific regulations to ICOs (e.g. AML, KYC, etc.) and see, at presence, no reason to regulate ICOs themselves.

5.6. Legal Context for Smart Contracts[17]

A smart contract is only a piece of software code without further legal relevance. Only if embedded in a legal context and confirmed by the parties, it can unfold and realize its potential and desired effects.

Private and autonomous contract parties can reach an agreement regarding clauses for every individual case. However, in order to support the acceptance and ease of use, it makes sense that the legislation determines such «smart contexts» which are valid for smart contracts and clarifies how such smart contracts are embedded in the current legal system. This is particularly true with regard to the avoidance of errors and to clarify how errors can be corrected, even if they are already written as a piece of software stored as block. The risk that unwanted action is executed by smart contracts against the will of *both* parties is too high.

5.7. Local Regulation vs. International Regulation

International attempts to regulate blockchains have started slowly. State specific regulation concepts still have priority. Since central banks see blockchains as a tool for themselves too, it is only a matter of time until international coordination and aligned standardization will start being developed[18]. The already mentioned

[16] FINMA-Aufsichtsmitteilung 04/2017, https://www.finma.ch/de/dokumentation/finma-aufsichtsmitteilungen.

[17] The author has developed a concept of «smart contexts» to support the development and validity of smart contracts. Cf. Ebenhoch/Gantner 2018.

[18] Henderson 2017.

Crypto Valley Association announced an ICO code of conduct which sets principles for ICOs in general[19]. Such approaches will pave the way for broader acceptance of specific blockchains applications and of ICOs.

6. How to Regulate Blockchain Regulation / a Plea for Human Rights

There is reasonable suspicion that China has banned cryptocurrencies and ICOs because it has understood the decentral power of blockchain applications[20]. The public utilization of blockchain power to establish a gapless surveillance state and the misuse of connected blockchains by monopolistic corporations to nudge and disenfranchise citizens should be an internationally shared and widely discussed concern.

The technical fascination to use blockchains to gain trust and clarity without intermediaries is impressive. However, getting aware of the heavy technological implications it seems to be very misleading, too. And if owned by the state and/or operated by monopolistic organizations, it can lead to an inhuman gapless surveillance of the worst sort, too. Clear legal guidance and compliance frames can and have to support the benefits.

The future will reveal to which extent intermediaries and the fuzziness of legal language is not only a burden, but also a resource of compensation, harmonization and a contribution to avoid conflicts. It will also show more clearly the shortcomings of technical consensus mechanisms compared to human-based methods.

7. References

Alloway, Tracy, An Experiment, 2017, http://www.tracy-alloway.com/?p=577.

Bheemaiah, Kariappa, The Blockchain Alternative, Apress, 2017.

Biederbeck, Max, Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen, Wired, 2016, https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde.

Brodu, Etienne, Blockchain, Degeneration of an Ideal, OuiShare Magazine, 2017, http://magazine.ouishare.net/2017/11/blockchain-degeneration-of-an-ideal/.

Chadwick, Sam, Crypto Valley Association Comes Out in Support for Careful ICO Regulation; Announces ICO Code of Conduct, Crypto Valley, 2017, https://cryptovalley.swiss/crypto-valley-association-comes-out-in-support-for-careful-ico-regulation-announces-ico-code-of-conduct/.

Chanyaporn Chanjaroen/Andrea Tan/Haslinda Amin, Singapore Won't Regulate Cryptocurrencies, Central Bank Chief Says, Bloomberg, 2017, https://www.bloomberg.com/news/articles/2017-10-24/singapore-won-t-regulate-cryptocurrencies-remains-alert-to-risk.

Ebenhoch, Peter/Gantner, Felix, Smart Contexts für Smart Contracts – Legal Programming für valide Blockchain-Verträge, in diesem Band, 2018.

Gerard, David, Attack of the 50 Foot Blockchain, CreateSpace, 2017.

Gourdan, Shidan, How Future Regulation Will Shape Canada's Blockchain Environment, Techvibes, 2017, https://techvibes.com/2017/12/15/how-future-regulation-will-shape-canadas-blockchain-environment.

Henderson, David, Blockchain Regulation in Europe and Potential Hurdles, Nasdaq, 2017, http://www.nasdaq.com/article/blockchain-regulation-in-europe-and-potential-hurdles-cm854360.

Kleinz, Torsten, Initial Coin Offerings: China verbietet Investmentform mit Kryptogeldtokens, Heise Online, 2017, https://www.heise.de/newsticker/meldung/Initial-Coin-Offerings-China-verbietet-Investmentform-mit-Kryptogeldtokens-3821656.html.

Hosp, Julian, War's das mit deinem Invest in Bitcoin? Regulierung der Blockchain wirft Fragen auf (Podcast), T3N, 2017, https://t3n.de/news/bitcoin-blockchain-regulierung-863540/.

[19] Chadwick 2017.

[20] Expressed by Dr. Julian Hosp, see Hosp 2017.