THE IMMUTABILITY CONCEPT OF BLOCKCHAINS AND BENEFITS OF EARLY STANDARDIZATION

Frank Hofmann[*] *, Simone Wurster*[*]*, Eyal Ron*[§] *and Moritz Böhmecke-Schwafert*[*]

[*]Chair of Innovation Economics Berlin University of Technology, Berlin - Germany

and [§]Cryptom Technologies UG, Berlin - Germany

ABSTRACT

The blockchain technology can be regarded as a groundbreaking invention with the potential to bring the digital revolution to the next stage by helping to realize peer economy solutions. The blockchain technology and the concept of blockchain immutability is discussed. The benefits of early standardization of the blockchain technology are argued based on the literature and the analysis of the central blockchain immutability characteristic. From this, a framework is proposed aimed at understanding the dimensions and boundaries of blockchain immutability. The resulting framework is suggested as a good practice standard for the implementation of blockchain systems. Based on these efforts, the article supports initiatives to better exploit the blockchain technology's full potential by standardization.

Keywords— blockchain, standard, immutability, peer economy

1. THE PEER ECONOMY AND THE ROLE OF THE BLOCKCHAIN TECHNOLOGY

The digital revolution has been heavily impacting organizations, economies and modern societies in the last decades ([1] p. 4-9). As one of the latest waves of IT innovations following social media, mobile devices, the internet as well as personal and mainframe computers in the last decades ([2] p. xii), the blockchain technology, spearheaded by the innovative Bitcoin application, has emerged as a potentially disruptive IT innovation [3][4][5].

The disruptive effects of the blockchain technology do not only concern business models by bringing intermediaries under competition, as it allows intermediary services without single trusted actors [6][7][8]. It has as well the potential to be an answer to the global change in markets driven by automation: Digitization is not just about the ubiquitous use of algorithms and ICT that revolutionize labor and consumer markets, but it also enables new opportunities in the form of IT-supported collaboration in the "peer economy" ([1] pp. 243): Tasks are split and sourced to a crowd instead of using well defined organizations. Peer-to-peer exchanges and collaboration between people allow them to crowd-participate in innovating markets ([1] pp. 241-247), to which the decentralization enabled by the blockchain technology offers a promising solution (see [2] p. 27, [4], [9], [10] p. 272). By virtue of immutable and redundantly held data records as well as distributed consensus mechanism, blockchains can further contribute to controlling the flood of digital data by providing common single reference points to share data and to evaluate key data (see [2] pp. 30-31, [4], [11]).

Following the introduction, the blockchain technology is presented and then discussed with the case of the "DAO wars". In the fourth chapter the need for early standardization of blockchain technology is elaborated. Subsequently, a framework is introduced in order to contribute to development of the technology by early standardization.

2. HISTORY AND CENTRAL CHARCTERISTICS OF THE BLOCKCHAIN TECHNOLOGY

The blockchain technology advent began in 2008 with the Bitcoin application. Following the publication of the Bitcoin whitepaper by Satoshi Nakamoto (pseudonym) in 2008 [12], the cryptocurrency Bitcoin was set up in 2009. It was used for the first time commercially in 2010 in order to purchase pizza for the price of 10,000 bitcoins [13]. From a price for a pizza order in 2010, the value of the 10,000 bitcoins rose until October 2017 to more than a 400,000 US$ (see [14]), illustrating Bitcoin's strong dynamics.

Soon after its launch, a wide array of further blockchain technology applications were developed ranging from so-called "colored coins" building on the Bitcoin blockchain [15] to new blockchain implementations such as Ethereum [16] or Hyperledger [17]. Currently, the blockchain tracking website coinmarketcap.com lists about 1,150 cryptocurrencies and other applications [18].

We propose, that a blockchain can be defined as "a distributed database that is practically immutable by being maintained by a decentralized P2P network using a consensus mechanism, cryptography and back-referencing blocks to order and validate transactions." [19].

A related term is "distributed ledger". It was found that both terms correlate and that, based on the last data of spring 2017, "blockchain" is the leading one [20]. There is however no clear consensus on the definitions yet, as a distributed database does not have to use blockchain technology [21]. For the purpose of this article, we consider the usage of the blockchain technology as defined, which is shortly described afterwards. At the core of blockchain technology is the decentralization of the database control ([6], [22] p. 219), which can be in its extent considered as a "revolutionary new computing paradigm" allowing a new level of coordination and collaboration ([2] p. 92).

The blockchain developer Richard G. Brown described the decentralization of trust (see [2] p. vii, [23]) as shifting the "trust boundary" from protecting a whole system against the outside by controlling access and centrally ensuring data validity, down to the individual participants in a blockchain network ([24], see also [12]). As blockchain network participants no longer need to trust each other or a third party to cooperate, dynamic online networks can form to share resources such as data and processing power or interact for different purposes in a peer to peer network.

A central property for the participants' trust in the blockchain is the immutability of the data records [3][11]. This means, that recorded data cannot be manipulated or modified after being accepted by the blockchain network. As discussed later in the case of the "DAO wars" and subsequent chapters, the concept of immutability is also extended to the rules and even the functions of blockchain applications by parts of the blockchain community.

The shift of the trust border to the individual user level is realized by technical principles of blockchain technology: Information is stored in a chain of data blocks, each of which references the preceding data block by an alphanumeric string derived from the preceding block (typically using a hash function), which makes it improbable to manipulate the data published in a block without being noticed, as the reference values would no longer fit the referenced data blocks ([10] pp. 64-65, [12]).

New data is integrated by a distributed consensus mechanism[1] leading to a convergence towards a commonly accepted state, which in the case of the Bitcoin blockchain means, that each participant creating data blocks selects the longest valid blockchain in order to attach new blocks ([10] pp. 65-68, [12]). The creation of blocks is for example in the Bitcoin blockchain, so-called "mining", is motivated by a block creation reward and transaction fees in bitcoins, but requires a processing of a power-costly cryptographic proof to demonstrate commitment and deter malicious behavior ([10] pp. 38-45 and 104-119, [12], see also [3]). This results in an agreement on a sequence of valid data blocks, with valid meaning for Bitcoin that the preceding data blocks are correctly referenced and are consistent with the rules and the (publicly visible) past Bitcoin transactions in the blockchain ([10] pp. 66-69).

The immutability of recorded data on a blockchain can be breached. A breach of immutability can occur due to bugs in the code (see e. g. [25], [26]) But breaching the immutability of recorded data is possible even in an idealized implementation of a blockchain, although it is considered in general (a) improbable or (b) extremely difficult.

(a) An improbable breach of immutability would occur, if one tried to attack the blockchain data structure of blocks chained by hashes. If it can be assured that it is improbable to find two blocks with identical hash value, mathematically called "collision resistant", then such an attack will not be possible in practice. While for each possible hash value theoretically an infinite number of blocks exists, for which a hash function gives this value, a well-defined hash function makes it improbable to find such two blocks even if a user is holding an unreasonably high amount of computational powers ([27] pp. 153-156). This principle has not yet been proven for the standardized CRSC hash functions [28], which are currently used in applications, but it is a strong belief of the community that this is the case ([27] pp. 231-236).

(b) An extremely difficult breach of immutability is one that requires a very large amount of resources to convey, but which is in principle possible. One example is an attack on Bitcoin's consensus mechanism: If one possesses a computational power which is higher than 50% of the computational power of the whole network, one can try to delete a transaction from the blockchain by sending a modified blockchain as consensus. Bitcoin's hash power sums up to more than 10,000,000 TH/s at the end of October 2017 [29], which means that about 740,741 units of one of the strongest miner (Antminer S9, 13.5 TH/s, 1265 dollars apiece as of 4th October, 2017, see [30] and [31]) are needed. This would cost around 937 million dollars not including electricity costs and other needed efforts.[2]

Therefore, and in all cases known to the authors, immutability was so far only breached by forks, meaning different distributed software versions of the same blockchain existing in parallel, as will be discussed in the case of the DAO in chapter 3. The ability to validate the recorded blockchain data and the authentication of users by encryption keys as digital signatures are as well central to form a decentralized consensus without the need to know and trust the participants in a blockchain network[3] [22][32]. There are also additional measures to be taken into account, e.g. to counter misbehavior and attacks. A more detailed and encompassing discussion of the technology can be found in [10][32][33].

Enabling new forms of peer collaboration and coordination and thus novel business models and applications, blockchain technology is attracting wide interest as shown in various implementations and applications (see [18], [34], [35]). As it is an emerging and still maturing technology, solutions are needed to clarify and standardize its basic terms and concepts, as the next chapter will demonstrate.

[1] Several versions of consensus mechanisms are developed for blockchains, see e.g. [3].

[2] Smaller networks may face higher risk, but may as well offer less incentives for would-be attackers.

[3] With the cryptographic keys the user input is authenticated - the anonymity is a design choice.

3. THE CASE OF THE DAO WARS

Besides its industry-wide publicity, the blockchain technology also experienced setbacks. Among the most prominent incidents were the one of the Bitcoin exchange Mt. Gox with a tremendous damage of $350m in Bitcoin cryptocurrency [36] and of the Ethereum-based "Decentralized Autonomous Organization" (DAO) with an initial damage of $50m in the cryptocurrency ether [37]. Such adverse events could jeopardize user trust in the blockchain technology significantly.

The latter case with the hack of the DAO or the so-called "DAO wars" caused fundamental discussions regarding the concept of immutability as a central characteristic of blockchains [38][39][40].

The DAO blockchain is one of the first attempts to form a decentralized crowd-funded organization on the Ethereum blockchain by which users can obtain shares by buying so-called DAO tokens [38]. These tokens give them proportional voting rights on the investment into specific projects and accordingly the corresponding economic rents [38]. The blockchain code and the immanent rules and automatisms were not supposed to be subjects of change and thus were regarded as "immutable" [40]. In June 2016, an attacker used a only recently noticed breach in the DAO code to appropriate tokens from other participants equivalent to about $50 million [37].

As the implemented code delayed payout, the DAO and Ethereum community had four weeks to react to "the attacker's" transfer. Due to the DAO's significance in the Ethereum ecosystem, a controversial discussion evolved within the blockchain communities, such as on the Reddit forum, whether to undo the breach exploitation in that time [38][41][42].

If the DAO were a traditional centrally managed organizational software, the common procedure would have been to solve the breach in the code and transfer the $50m back to its original owners. However, the DAO structure building on blockchain technology requires a network consensus on how to proceed [38][39].

One view point advocated a correction of the Ethereum protocol to fix the consequences of the breach in the DAO code. The second most prevalent view of the community argued, that there should be no ex-post modification as undoing the manipulations would be a violation of the "immutability principle", which sees the code as the single point of truth [38][39].

In the end the majority decided on a protocol correction resulting in a split into two different Ethereum blockchains, breaching the immutability by a fork [38], but without solving the discourse about the perception of blockchain immutability. The "DAO wars" have shown, that the central attribute immutability is not commonly understood within the blockchain developer community.

Besides others incidents, this revealed the ambiguity of blockchain concepts in the field of blockchain technology. Misconceptions like these challenge the future development and jeopardize trust in such blockchain solutions significantly.

It is also noteworthy, that the principle of using blockchain tokens for investments, so-called "initial token offerings" (ICO), is a popular financing method for blockchain start-ups, which underlines the significance of clarifying the concept of immutability.

We argue, that this issue can be addressed by appropriate standards specifying fundamental blockchain terms, concepts and characteristics, an appropriate business to customer communication regarding these characteristics as well as regarding the resulting rights and duties on the side of the blockchain developers and users. Following the need for early standardization revealed by the case of DAO, the benefits of early standardization will be argued in the next section.

4. NEEDS AND CHALLENGES FOR EARLY STANDARDIZATION OF BLOCKCHAINS

Standards play a central role for industrial societies and international technology systems [43]. They can be understood as a consensual, public document from a recognized institution for the "achievement of the optimum degree of order in a given context." ([44] p. 12). In addition, besides consolidated scientific and technological contributions, standardization also considers learning from practitioner experiences to optimize community benefits from standards [44].

According to [45][46], four categories of standards can be distinguished:

- semantic standards,
- measurement and testing standards,
- interface standards and compatibility standards and
- quality standards and variety-reducing standards.

Regarding the product life cycle, [47] identified three types of standards: Anticipatory, participatory, or responsive standards. Anticipatory standards are standards "that must be created before widespread acceptance of devices or services". Participatory standards "proceed in lock-step with implementations that test the specifications before adopting them" and responsive standards "occur to codify a product or service that has been sold with some success" ([47], p. 2).

This paper refers to participatory standards, although it could be argued, that the suggested framework as well as consortia efforts or some international standardization committees have an anticipatory character as well, since they set the road for a broader implementation. It is directed as a quality standard towards supporting technology diffusion and acceptance.

Regarding innovative areas, the benefits of standards may refer, for example, to R&D and the diffusion of innovation, the time-to-market of new products, support for the technology transfer and the creation of critical mass (see [48], [49] for overviews of the advantages of standardization).

Besides the long list of advantages, which standards may provide, they can also introduce risks, such as monopoly power, regulatory capture and raising costs of competitors or reduced choice on markets [48]. An example of how to mitigate the risks is given in [50]. [48] explicitly emphasizes the positive influence of standards on innovations as well. Likewise [46] shows various benefits that standardization of an emerging technology such as the blockchain field can achieve. As the understanding of the very concept of what a blockchain is still ambiguous (see [51], [52], [53]), early standardization efforts could help significantly to clarify mutual understanding.

It is found in [54], that users are willing to use a blockchain, if the blockchain technology is easy to use concerning both the technological and business side, useful in terms of effectivity and efficiency benefits and incurs only acceptable risks regarding security, privacy or stability. Trust impacts these user assessments [54] and standards can support both the evaluation of a blockchain application as well as the trust in the technology itself.

In line with these considerations, [55][56] specify as the current needs for standardization reference architecture, taxonomy as well as ontology. In that respect, the concept of the immutability concerns both taxonomy and ontology of blockchains. [57] adds, that international standards, standards that assist a new emerging technology to be rolled out and deployed with greater clarity, certainty and market confidence, shared solutions for customer requirements as well as for smart contracts are important.

According to [57], leading standardization organizations, in particular, ISO, ITU and CEN respond to these needs. ISO for example, created a roadmap, covering a three year period between April 2017 and April 2020. Key issues, addressed by ISO working groups and study groups, include "Terminology", "Taxonomy / Reference Architecture", "Identity", "Interoperability", "Governance", "Security & Privacy", "Use Cases" and "Smart Contracts".

Additionally, large industry-supported consortia such as Hyperledger Fabric of the Linux Foundation have been evolved to develop modular blockchain solutions [58][59].

This article adds to these efforts by (a) introducing and explaining the fundamental blockchain immutability characteristic in chapter 2 and 3 as well as (b) suggesting an appropriate user and investor communication as well as management of this characteristic in the next chapter.

In line with the findings of [56][57], it is essential that the recorded data and the rules of cooperation in the blockchain network are reliable for the participants to trust the network. This requires a clarification of its immutability characteristics, respectively the conditions under which the active blockchain can be modified (see [42]) furthering trust and customer confidence. The question has thus to be posed, under which circumstances should a blockchain be subject to modifications, while at the same time ensuring a non-manipulable consistent consensus between the networks' participants. To achieve consensus, but also to incorporate the user requirements, the early involvement of all stakeholders is critical in defining such requirements.

5. SUPPORT OF TECHNOLOGY USAGE BY MANAGMENT OF IMMUTABILITY

A remarkable characteristic of the blockchain evolution is its technology development in open as well as distributed communities. The knowledge exchange is driven by the sharing of whitepapers and realized often informally or even anonymously by means such as forums and blogs or face-to-face discussions and conferences (see also [60], [61]).

The dynamic, large and varied field of proposed blockchain solutions makes it also difficult to accurately pinpoint the benefits of the proposed and typically unproved solutions. Taking as well the immature state of the technology and ambiguity of concepts into account as discussed before, the development of the blockchain technology can be described as chaotic. In [53] an approach to define terms for the complex blockchain technology development is proposed. However, as the DAO case has shown, the central role of immutability requires further considerations.

Consequently, guiding quality standards for operation and implementation are needed to better handle the chaotic technology development. Supplementing committee discussions on term definitions to promote common understanding, on references to compare and test, or on data exchange specifications for compatibility, the presented framework focuses on the system aspect of the blockchains and the support of its management.

In the following, an approach to clarify the principles of blockchain immutability is proposed as a participatory quality standard to support the roll-out and deployment by clarifying the central concept of immutability and its management for operations. With a layered framework, the implementation of immutability is made manageable for blockchain developers and users.

The immutability concept concerns both the data and the code of the blockchain as discussed before. The immutability of the data is generally seen as an uncontroversial aspect realized by the technical properties of the blockchain data structure as discussed in chapter 2.

It has to be pointed out, that blockchain solutions have limits in what they can achieve: While immutability of recorded data may be ensured, the data may be erroneous before entry into the blockchain. The consensus system may be used to verify entry data, but this has limits in what the participants can reliably deliberate and consent on (see [62]).

The immutability of the code is however a highly controversial concept, as shown in the DAO case in chapter 3. No code is created in perfect state integrating all operative requirements from the start. A blockchain code has to be, and in all popular cases known to the authors is, continuously adapted. For a distributed consensus system, there are differences in how far users are affected by a code change. Adding a function for comfort, fixing a bug or improving the handling of a data format has a different impact for the users than changing the rules of the system that concern trust: The privileges of data integration, the miner incentives, the consensus finding system and so on.

As discussed beforehand, the blockchain technology still has technological issues such as scalability, security, privacy, functionality, efficiency and reliability that needs to be improved ([63], [64], [65], [66], [67], [68], [69]) making software updates necessary. An update would be successful, if the blockchain network participants use the new code and drop the outdated code version. The acceptance is of critical concern, as it has the potential to cause inconsistent and incompatible versions to coexist (forks), divide the network and impact trust. From the impacted users' perspective, a blockchain code could be modified in several ways assuming the required IT infrastructure to operate the network as given:

(a) The software code could be modified to improve the code execution or remove specific weaknesses without altering key properties (e.g. "Performance Improvements" in [70] or "Test for LowS signatures" in [71]).[4] Users can simply acknowledge such changes.

(b) The software code could be modified to offer additional functions concerning data administration (e. g. "Standard script rules relaxed for P2SH addresses" in [72] or "Block file pruning" in [73]).[5] Users have to inform themselves about the new possibilities or potential limitations.

(c) The software code modification could alter or affect key blockchain network properties (e. g. the discussed "correction" of the DAO hack or an update to the cryptographic proof of work in the Bitcoin blockchain as discussed in [74]). In such cases, users need to review the changes and consent to them.

The presented framework takes the distinctive perspective of the network participants, who have to place their trust in the system, to help manage the inherent conflict within the concept of conditional immutability of a blockchain. From the described differences in impact on the system users, four layers are derived (see figure 1):

(1) The execution layer at the bottom of figure 1 represents the software code execution running locally on the users' hardware and that operates on the IT infrastructure. It forms the basis for the following layers. Changes on this layer are performance, stability or security improvements. They do not alter functionalities for participants, carried data, network properties or consensus mechanism as experienced by the users.

If well documented and transparent, e. g. as blog entries on a regular schedule, such changes are part of the maintenance work and will not in general negatively impact the trust of the users.

(2) The function layer concerns the related functions allowing the users to work with the data. Changes on this layer between local execution and system layer may be a concern for trust and consistency, as decisions to cut or add data may concern central blockchain properties such as historical completeness. On the other side, additional functions to implement a contract or function to check data may not be a great concern for trust, but part of regular application development, which needs to be communicated.

Therefore, functional changes have to be verified for their system impact and if necessary handled purely under the system layer. In case neither data nor system rules are changed, the changes can be handled as code updates. Changes only on the function and execution layer can and will typically occur frequently and are not of concern for the immutability of a blockchain.

(3) The system layer concerns the users' interactions with the blockchain on the network level, respectively system properties such as participation incentives, encryption, anonymity, consensus mechanism or network permissions. Changes on this layer require common understanding within a peer network about the specific modalities of the modifications (if, when and how) before implementation, as they have the potential to affect common agreement and subsequently trust so strongly, that they can cause network splits as demonstrated by the "DAO wars" (see chapter 3).

They should be clearly marked and communicated well in advance to allow a sufficient discussion. Even more important is however, the predefinition of the modalities for such cases to set a clear frame for the handling. Changes on the system layer are thus to be considered possible, if the conditions for them are described and agreed in advance. Due to this, system properties are only conditionally immutable. The conditions are of interest to users, investors and regulators and have to be published upfront ideally within the first whitepaper and.

(4) The data layer concerns the data stored on the blockchain and thus data immutability, as any non-consensual changes of data violates the historic consistency and completeness of the blockchain. In general, data is only added and there are no conditions under which data on the blockchain can be removed. The historic data is to be seen as immutable. It has to be noted however, that it can be temporarily uncertain, whether data is already consensually accepted depending on the duration of the convergence process in the distributed blockchain network.

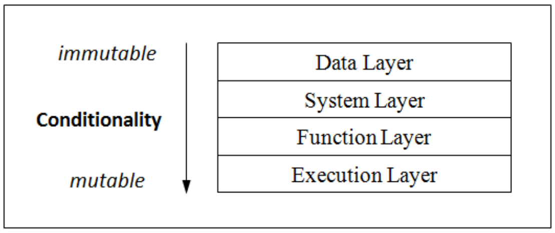

Figure 1: Layers of blockchain immutability

The potential impact of changes on the blockchain network participants has to be carefully considered and clearly communicated depending on the corresponding layer in the

[4] Due to technical reasons downward compatibility may be broken in some cases, which can lead to divisions.

[5] Note that a change in data management does not have to be contrary to blockchain data immutability.

framework. As a quality standard, the developers should specify any potential changes corresponding to the four levels, their conditionality (if, when and how) and their possible impact in detail upfront based on the proposed framework to increase trust and promote the diffusion of the technology.

A suitable mechanism of how to agree on proposed changes on the system layer would depend on the type of blockchain and its consensus mechanism.

The "immutability of a blockchain" is thus in general the immutability of its recorded data and the conditional immutability of its system rules and properties. The disclosed conditionality of changes to blockchain network properties can be seen as the constitution of a decentralized organization, which is realized by a blockchain.

As a final comment, the so-called smart contracts, which are in principle program code distributed with the blockchain, offer powerful possibilities to work with data on blockchains depending on inputs and are in general part of the function layer. The blockchain system does only guarantee the validity of them as far as the consensus or automated checks validate their properties and results. Their power to affect data or system properties should be clearly described and checked.

6. CONCLUSION AND OUTLOOK

Blockchain technology has the potential to become a cornerstone of the digital revolution by enabling decentralized cooperation in networks, when technological development continues to address user requirements. The development of early standards and good practices can also offer fundamental support for the technological development and its market acceptance.

An essential network property is the trust placed in the recorded data respectively transactions as well as in the rules of the decentralized network. As a result, the ambiguous concept of immutability has evolved in the blockchain community, but remained elusive as discussed in the DAO wars case. To ensure the success of the blockchain technology field, we have discussed the need for quality standards specifying good industry practice. The whitepaper documentation of blockchain solutions should describe clearly the conditions under which code or even system rules may yet change. For this purpose a classification has been provided to support maintenance and updates, while specifying the system property of immutability.

When the decentralizing and coordinating potential of the blockchain technology can be successfully exploited, applications in many fields such as in the manufacturing sector, the financial service sector, the health sector, E-government or the internet of things may be realized and drive a wave of economic and social changes (see also [2] pp. 101-104).

To support this development standardization has been recognized as an important topic.

Continuing research should address especially technical short-comings to improve usability of the technology, the competitive implementation of specific use cases to demonstrate its potential as well as economic and legal aspects to clarify user benefits for the different types of blockchains and to reduce market uncertainty about future regulation.

In addition, the development of crowd-sourcing and collaboration applications using the blockchain technology should be further investigated.

REFERENCES

[1] Brynjolfsson, Erik, and Andrew McAfee. *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. WW Norton & Company, 2014.

[2] Swan, Melanie. *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 2015.

[3] Mattila, Juri. "The Blockchain Phenomenon - The Disruptive Potential of Distributed Consensus Architectures." *Berkeley Roundtable of the International Economy Working Paper* 2016-1, 2016.

[4] Wright, Aaron, and Primavera De Filippi. "Decentralized blockchain technology and the rise of lex cryptographia." *Available at SSRN*, 2015.

[5] Allen, Darcy WE. "Blockchain Innovation Commons." *Available at SSRN*, 2017.

[6] MacDonald, Trent J., et al. "Blockchains and the boundaries of self-organized economies: Predictions for the future of banking." *Banking Beyond Banks and Money*. Springer International Publishing, pp. 279-296, 2016.

[7] Lee, Larissa, "New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market." *Hastings Business Law Journal* 12, Issue 2, pp. 81-132, 2016.

[8] Kiviat, Trevor I. "Beyond Bitcoin: Issues in Regulating Blockchain Transactions." *Duke Law Journal* 65, pp. 569-608, 2015.

[9] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." *IEEE Access* 4, pp. 2292-2303, 2016.

[10] Narayanan, Arvind, et al. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[11] Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." *Applied Innovation* 2, Berkeley.edu, pp. 6-19, 2016.

[12] Nakamoto, Satoshi. Bitcoin: *A peer-to-peer electronic cash system*. www.cryptovest.co.uk, whitepaper, 2008.

[13] Zohar, Aviv. "Bitcoin: under the hood." *Communications of the ACM* 58.9, pp. 104-113, 2015.

[14] http://www.coindesk.com/price (visited on 05.10.2017).

[15] Rosenfeld, Meni. *Overview of colored coins*. bitcoil.co.il, whitepaper, 2012.

[16] Buterin, Vitalik. *A next-generation smart contract and decentralized application platform*. ethereum.org, whitepaper, 2014.

[17] https://www.hyperledger.org (visited on 05.10.2017).

[18] http://coinmarketcap.com/all/views/all (visited on 04.10.2017).

[19] DIN SPEC Draft. "Blockchain Terminology." *DIN SPEC (PAS) 16597 Draft version from the 02.10.2017*, 2017.

[20] Tasca, Paolo. "Blockchain/DLT standardisation workshop – Introduction to the Blockchain/DLT and Terminology." *EC. Blockchain and Distributed Ledger Technology policy and standardisation workshop*, 2017.

[21] Walport, Mark. "Distributed ledger technology: beyond block chain." *UK Government Office for Science*, 2016.

[22] Böhme, Rainer, et al. "Bitcoin: Economics, technology, and governance." *The Journal of Economic Perspectives* 29.2, pp. 213-238, 2015.

[23] Atzori, Marcella. "Blockchain technology and decentralized governance: Is the state still necessary?" *Available at SSRN*, 2015.

[24] https://gendal.me/2016/11/08/on-distributed-databases-and-distributed-ledgers (visited on 05.10.2017).

[25] https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md (visited on 05.10.2017).

[26] https://blog.ethereum.org/2016/11/25/security-alert-11242016-consensus-bug-geth-v1-4-19-v1-5-2 (visited on 05.10.2017).

[27] Katz, Jonathan and Yehuda Lindel. *Introduction to Modern Cryptography*. CRC Press, 2014.

[28] https://csrc.nist.gov/projects/hash-functions (visited on 05.10.2017).

[29] https://blockchain.info/charts/hash-rate (visited on 05.10.2017).

[30] https://www.buybitcoinworldwide.com/mining/hardware (visited on 05.10.2017).

[31]https://shop.bitmain.com/productDetail.htm?pid=000201709281019141777wvS8I1g068C (visited on 05.10.2017).

[32] Badev, Anton, and Matthew Chen. "Bitcoin: Technical Background and Data Analysis." *Finance and Economics Discussion Series* No. 2014-104, Federal Reserve Board, Washington, D.C., 2014.

[33] Antonopoulos, Andreas M. *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc., 2014.

[34] Buehler, Kevin, et al. "Beyond the Hype: Blockchains in Capital Markets." *McKinsey Working Papers on Corporate & Investment Banking* No. 12, 2015.

[35] Evans-Greenwood, P. et al. *Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality*. Centre for the Edge, Deloitte Australia, 2015.

[36] Umeh, Jude. "Blockchain Double Bubble or Double Trouble?" *ITNOW*, pp. 58-61, 2016.

[37] O'Shields, Reggie. "Smart Contracts: Legal Agreements for the Blockchain" *N.C. Banking Institute* 21.1, 2017.

[38] Tosovic, Vladimir. *Der DAO-Hack – und die Konsequenzen für die Blockchain in Blockchain Technology - Einführung für Business- und IT Manager*. Ed. by Burgwinkel, Daniel, De Gruyter Oldenbourg, pp. 159-165, 2016.

[39] https://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb (visited on 05.10..2017.

[40] https://medium.com/@Swarm/daos-hacks-and-the-law-eb6a33808e3e (visited on 05.10.2017).

[41] https://www.reddit.com/r/ethereum/search?q=DAO-Hack&sort=relevance&t=all (visited on 05.10.2017).

[42] http://cryptom.site (visited on 05.10.2017).

[43] Blind, Knut, and Andre Jungmittag. "The impact of patents and standards on macroeconomic growth: a panel approach covering four countries and 12 sectors." *Journal of Productivity Analysis* 29.1, pp. 51-60, 2008.

[44] ISO/IEC. "Standardization and related activities — General vocabulary." *ISO/IEC GUIDE 2:2004(E/F/R),* 2004.

[45] Gauch, Stephan. "Towards a theoretical assessment of the link between research and standardisation." *Proceesings of the 11th EURAS Workshop on Standardisation. Hamburg, European Academy for Standardization, Aachen: Wissenschaftsverlag Mainz (Aachener Beiträge zur Informatik 38)*, 2006.

[46] Blind, Knut, and Stephan Gauch. "Research and standardization in nanotechnology: evidence from Germany." *The journal of technology transfer* 34.3, pp. 320-342, 2009.

[47] Sherif, Mostafa H. "Contribution towards a theory of standardization in telecommunications." *1st IEEE Conference on Standardisation and Innovation in Information Technology, Aachen,* 1999.

[48] Swann, G. M. Peter. *The Economics of standardization. Final Report for Standards and Technical Regulations Directorate Department of Trade and Industry*. Manchester Business School. Manchester, 2000.

[49] Wurster, Simone. *Born Global Standard Establishers. Einfluss- und Erfolgsfaktoren für die internationale Standardsetzung und Erhaltung.* Wiesbaden, Gabler, 2011.

[50] Blind, Knut. (2009). "Standardisation: a catalyst for innovation." *Inaugural Address Series Research in Management*. Erasmus Research Institute of Management. Rotterdam, 2009.

[51] Deshpande, Advait, et al. "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards." *Overview report The British Standards Institution (BSI)*, 2017.

[52] de Kruijff, Joost, and Hans Weigand. "Towards a Blockchain Ontology." *Research report Tillburg University*, 2017.

[53] Wurster, Simone, et al. "Standardisierung einer Terminologie für Blockchains – Spezifizierung der Grundlagen eines neuen Technologiegebiets." *DIN Mitteilungen +Elektronorm* 8-2017, Beuth Verlag, pp. 17-23, 2017.

[54] Folkinshteyn, Daniel and Mark Lennon. "Braving Bitcoin: A technology acceptance model (TAM) analysis." *Journal of Information Technology Case and Application Research*, 18.4, pp. 220-249, 2016.

[55] Abeloos, Benoit and Roman Beck. "Standardisation needs on use cases." *EC. Blockchain and Distributed Ledger Technology policy and standardisation workshop*, 2017.

[56] Ozcan, Christophe and Sylvain Cariou. "Standardisation needs on Reference Architecture, Taxonomy, and Ontology." *EC. Blockchain and Distributed Ledger Technology policy and standardisation workshop*, 2017.

[57] Abeloos, Benoit and Gilbert Verdian. "Blockchain/DLT standardisation workshop– Strategic Plan*." EC. Blockchain and Distributed Ledger Technology policy and standardisation workshop*, 2017.

[58] Martin Valenta and Philipp Sandner. "Comparison of Ethereum, Hyperledger Fabric and Corda." *FSBC Working Paper June 2017*. Frankfurt School Blockchain Center, 2017.

[59] Cachin, Christian. "Architecture of the Hyperledger blockchain fabric." *Workshop on Distributed Cryptocurrencies and Consensus Ledger,* Zürich, 2016.

[60] Allen, Darcy WE. "Discovering and developing the blockchain cryptoeconomy." *Available at SSRN*, 2016

[61] Lindman, Juhoet al. "Opportunities and Risks of Blockchain Technologies: A Research Agenda." *50th Hawaii International Conference on System Sciences* January 2017, 2017.

[62] Lemieux, Victoria Louise. "Trusting records: is Blockchain technology the answer?" *Records Management Journal* 26.2, pp. 110-139, 2016.

[63] Luther, William J. and Lawrence H. White. "Can Bitcoin Become a Major Currency?" *George Mason University Department of Economics Working Paper* No. 14-17, 2014.

[64] Bentov, Iddo, et al. "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract] y." *ACM SIGMETRICS Performance Evaluation Review* 42.3, pp. 34-37, 2014.

[65] Kraft, Daniel. "Difficulty control for blockchain-based consensus systems." *Peer-to-Peer Networking and Applications* 9.2, pp. 397-413, 2016.

[66] Croman, Kyle, et al. "On scaling decentralized blockchains." *International Conference on Financial Cryptography and Data Security*. Springer Berlin Heidelberg, pp. 106-125, 2016.

[67] Giechaskiel, Ilias, et al. "On Bitcoin Security in the Presence of Broken Crypto Primitives." *ESORICS 2016*, 2016.

[68] Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." *Security and privacy in social networks*. Springer New York, pp. 197-223, 2013.

[69] Yli-Huumo, Jesse, et al. "Where Is Current Research on Blockchain Technology?—A Systematic Review*." PloS one 11*.10 (2016): e0163477.

[70] https://bitcoin.org/en/release/v0.14.0 (visited on 05.10.2017).

[71] https://bitcoin.org/en/release/v0.10.3 (visited on 05.10.2017).

[72] https://bitcoin.org/en/release/v0.10.0 (visited on 05.10.2017).

[73] https://bitcoin.org/en/release/v0.11.0 (visited on 05.10.2017).

[74] https://news.bitcoin.com/bitcoin-developers-changing-proof-work-algorithm (visited on 05.10.2017).