AN EXPLORATIVE PAPER ON SPECULATIVE APPROACHES TO SMART CONTRACTS

Sanel Halilbegovic[a], Necip Ertem[a]

Abstract

The trend of cryptocurrencies has stirred interest in the underlying technology that qualifies cryptocurrencies as a secure structure with speedy, timely and cheap transactions. The aforementioned technology, the blockchain, in brief terms is a decentralized ledger technology that attains an immutable characteristic through consensus and timestamp mechanics. The model also sets the stage for transparency in transactions, which renders the technology applicable to a myriad of scenarios that involve financial instruments. This research puts forth an argumentative approach to the applicability of blockchain technology and specifically studies the prospect of utilizing smart contracts. This approach probes the feasibility of introducing smart contracts to everyday financial transactions and settlements. An opposing perspective, by taking a devil's advocate standpoint, invokes the impractical or implausible aspects of implementing the blockchain in certain scenarios. Difficulty in auditing is a prominent example among those impracticalities. Research methodology is qualitative in nature and takes the form of exploratory research by examining existing literature on the topic.

Keywords: Smart contracts, trust mechanisms, transparency in transactions, big data
JEL Classification: D53, G23, E42

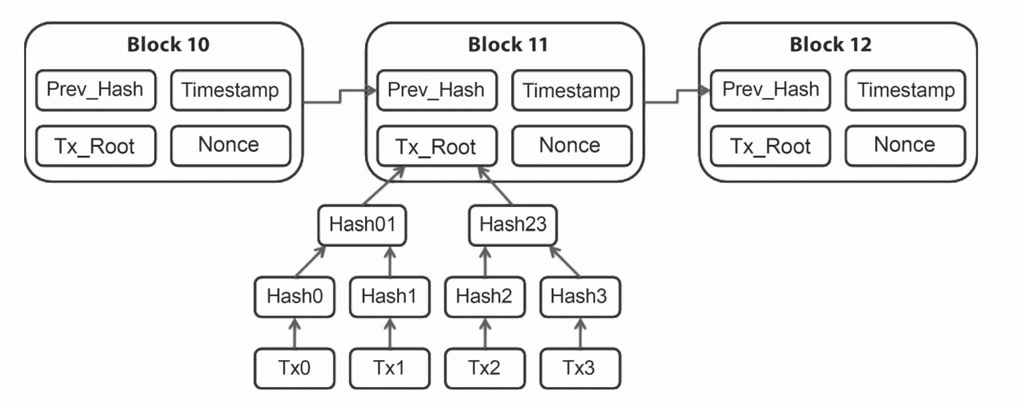
1. Introduction

Third-party brokerage in day-to-day transactions, as well as in sophisticated arrangements, has been a quintessential part of our financial system. When an individual seeks to purchase a product from the internet, this transaction is intermediated by a third party, namely a bank. These third parties are almost ubiquitous in financial areas when arbitrating the exchange between the customer and the seller. In many of these areas, fintech start-ups have sought to target the end customer directly, and the blockchain provides an evident opportunity

[a] International Burch University, Sarajevo, Bosnia and Herzegovina.
Email: sanel.halilbegovic@ibu.edu.ba, necip.ertem@stu.ibu.edu.ba

for that (Dietz *et al.*, 2016). The main reason why the blockchain is touted to obviate the need for financial intermediaries resides in its decentralized structure. This mechanism can be viewed as a public ledger of all transactions that have ever been executed (Fanning and Centers, 2016). This structure is principally attained through node consensus and block mechanisms that verify the propriety of the information. Each block is built upon the previous block and contains hash data from the preceding block as depicted in Figure 1. The data are recorded in chronological order in a manner that irreversibly timestamps every transaction (Narayanan *et al.*, 2016). Once a change is made in any of the blocks, this action invalidates all the blocks that come after it. Immutable, transparent and decentralized, this novel architecture has created fields of opportunities in applying the technology. Smart contracts are often pronounced among those prospects.

Figure 1: Blockchain example



Source: Google

A smart contract is fundamentally a digitalized contract that enforces the provisions of an agreement and if necessary exacts payment. Embedding them into the blockchain makes them self-executing; thus, they eliminate third-party intermediation in transactions, thereby reducing costs and saving time. Certain qualities make it one of the most sought-after technologies in finance: it reduces risk of non-payment and fraud, and imbues financial contracts with a certain degree of trust independent of that provided by an intermediating party.

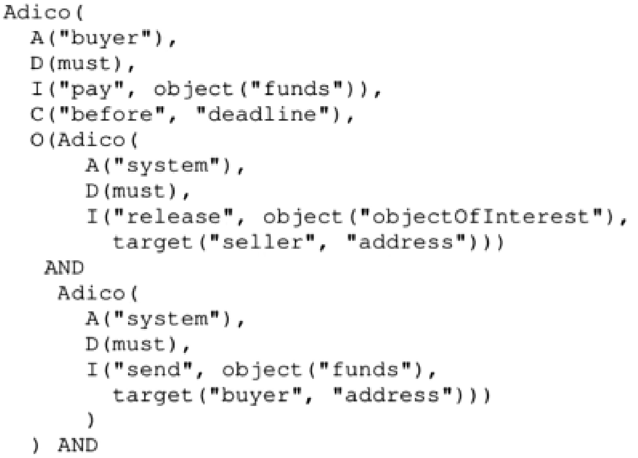
The aim of this research is to assess the feasibility and practicability of smart contracts. Along with its often-cited benefits, smart contracts are hard to exert any control over, which thereby might create problems in auditing, transparency and vulnerability. Interpretation of contractual terms by a machine is a technology beyond cryptocurrency and has remained without precedent to date. This research studies existing literature on the matter and interprets scalability of smart contracts in real life based on said materials.

2. Literature Review

We examine two types of literature on smart contracts. First we examine existing literature on smart contract problems and vulnerabilities, then we study previously published papers on the notion of trustless contracts and scalability concerns. Existing literature on main problems with smart contracts specifies numerous issues related to security and technical processes. The technical process category is inextricably linked with security as it shapes the integrity of the latter. Moreover, the following sections demonstrate that problems in security are often caused by deficient programming. Delmolino *et al.* (2015) specify difficulties in programming smart contracts into the blockchain. They argue that smart contracts require taking an "economic thinking" perspective and should be written diligently since they are susceptible to manipulation. Atzei *et al.* (2017) further elucidate vulnerabilities in Ethereum-based smart contracts and list certain functional issues by providing real-life problems that occurred with smart contracts, such as execution fees and programming gaps. The DAO attack is a prominent example here in which an attacker moved 60 million dollars worth of tokens to another account (Siegel, 2016). The case evokes risks of centralization, whereby a malicious third party takes control of a majority of the nodes (Tikhomirov, 2017). DDoS attacks on the mining pools – where the attacker seeks to undermine the success of a competing pool (Johnson *et al.*, 2014) – also pose a threat. To eliminate these issues, certain researches propose frameworks to analyse and verify the safety and functional correctness of Ethereum-based smart contracts (Bhargavan *et al.*, 2016). Another proposition is to write smart contracts in a way that allows system interaction and represents a humanly readable format (Frantz and Nowostawski, 2016). Marino and Juels (2016) propose a theoretical framework for terminating or modifying a smart contract whenever there is a discrepancy or conflict in the agreed terms, or when the code is faulty. This is strikingly difficult as data stored in a blockchain are distributed to all the nodes in a network in a manner that renders this action irreversible.

Another element that implicates the technical category of smart contracts is indubitably the material aspects of smart contract applications. The extreme level of energy consumption by the Bitcoin network was estimated at 2.55 GW in 2018 and was expected to rise above 7 GW in near future, which is on a par with the consumption of some European countries such as Austria (De Vries, 2018). Ethereum networks consume energy at a similar rate; smart contracts becoming widespread would bring about a similar issue.

Figure 2: Semi-automated code



```
Adico(
  A("buyer"),
  D(must),
  I("pay", object("funds")),
  C("before", "deadline"),
  O(Adico(
      A("system"),
      D(must),
      I("release", object("objectOfInterest"),
        target("seller", "address")))
   AND
    Adico(
      A("system"),
      D(must),
      I("send", object("funds"),
        target("buyer", "address")))
      )
  ) AND
```

Source: Frantz and Nowostawski (2016)

Tikhomirov (2017) states that the exorbitant energy consumption during mining is one of the problems with implementing the blockchain to smart contracts. It is worth noting here that the Proof-of-Work (PoW) concept is what entails these high energy consumption levels, which is why the Ethereum blockchain aims to switch to a hybrid PoS-PoW model (Hertig, 2017). In the Proof-of-Stake model, the creator of a new block is determined based on a stake where the power is distributed to miners based on their stakes (Bentov *et al.*, 2017). The energy consumption is eliminated by this concept, but the paradigm entails difficulties of its own. Tikhomirov (2017) identifies these problems as:

- *Nothing-at-stake problem:* Since PoW is no longer required, validating transactions does not put anything at stake; hence, validators rationally seek to extend to all existing chains.
- *Randomness of selecting validators:* The protocol by which the system selects the validator and the selection mechanism pertaining to that hash solution.
- *Transaction finality:* In the PoS method, choosing validators and producing blocks are two different events, contrary to PoW concurrent block header validation and block production.

Security concerns within smart contracts apart from the aforementioned drawbacks are as follows: *timestamp dependency, transaction-ordering dependency, mishandled exceptions and reentrancy* (Luu *et al.*, 2016).

- *Transaction-ordering dependency* occurs when one transaction in a contract is executed before another where both transactions exist in the same block. Consider the example of a puzzle that rewards the users whenever a solution is proposed. The miner can monitor the user responses and alter the execution order when there is an unprocessed transaction containing a valid submission, effectively succeeding in the attack.
- *Timestamp dependency* occurs when the execution of the contract is bound to the block timestamp. Since blockchain networks are asynchronous and the contracts are set according to the local miner's time zone, they are prone to manipulation by a colluding miner from that time zone.
- *Mishandling exceptions:* smart contracts written in Solidity also include exception protocols; therefore, if an exception is present and if the exception is not propagated to the called contract, the contracts are handled improperly (Luu *et al.*, 2016).
- *Reentrancy* is a prevalent issue which demonstrated itself in the DAO attack. Seijas and McAdams (2017) illustrated this problem in an example where a "withdraw" function retrieves money from an account by sending it to the user and receiving it from the balance. An attacker could repeatedly execute this function and withdraw funds from the balance.

Further research into the topic leans on scalability of smart contracts and albeit published papers are far fewer, the idea of smart contracts is thoroughly analysed. Furthermore, we include research that challenges the idea of trust-free contractualization. Giancaspro (2017) tackles smart contract scalability in a juridical context and states that "[i]t is uncertain whether they will easily adapt to current legal frameworks regulating 'conventional' contracts across jurisdictions." Gatteschi *et al.* (2018) argue that the technology, although very promising, needs maturing before implementation. Tikhomirov (2017) stated that the blockchain deliberately sacrificed performance for scalability. As Chu and Wang (2018) stated: "To achieve scalable execution of smart contracts, it is time to rethink the design of both the programming model and the runtime."

3. Research Methods

Only secondary web resources were used in conducting this research. Conference papers, articles, books, journals and magazines published between 2015 and 2018 were queried using Google Scholar and ScienceDirect. Keywords such as "problems", "setbacks", "weaknesses", "vulnerabilities" etc. were individually included under the keywords "smart contract" and "blockchain" to narrow down the query to relevant results. An initial screening was done by reading the titles of the query results. The primary elimination criteria were relevance to smart contracts (1) and whether the studies manifested drawbacks and disadvantages of smart contracts (2). Results were included indiscriminately regardless of the blockchain platform. The queries aimed to answer the following research questions:

RQ1: What are the problems and the respective solutions associated with those problems in smart contract applications?

RQ2: Are smart contracts, in all aspects, feasible or pragmatic as an improvement to existing mechanisms?

Table 1: Query results

	Google Scholar	ScienceDirect
Initial query results	389	161
Results after screening	44	15

Source: authors

The secondary screening process was done by reading the abstracts and conclusion sections of the studies remaining after the initial screening. This process narrowed the number of results down to 28 after duplicate studies were removed. Fourteen of the 28 studies analysed vulnerabilities, scalability problems, security concerns and most proposed frameworks or theoretical models to either detect vulnerabilities or improve the scalability and performance of smart contracts. Three of the studies presented contemporary knowledge and positions on smart contract utilization. The remaining twelve studies were essentially the foundation for the answers provided to RQ2.

Table 2: Study name, type and channel

Study name	Study type	Channel	Content
Is a 'smart contract' really a smart idea? Insights from a legal perspective (Giancaspro, 2017)	Computer law and security review	Journal/ Magazine	Questions the legal aspects of smart contracts across different jurisdictions.
The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy (Hawlitschek *et al*., 2018)	Literature review	Journal/ Magazine	Smart contracts in theory could be trust-free for tech-savvy users, but regular people have to trust the algorithm or the people creating the algorithm.
Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? (Gatteschi *et al*., 2018)	Research article	Journal	Weighs the benefits and drawbacks of the application of blockchain technology in the insurance sector with the caveat that the technology is yet to mature.
Not-So-Smart Blockchain Contracts and Artificial Responsibility (Kolber, 2018)	Tech review	Journal	Code ambiguities caused by semantics of the code, problems that lie within the irrevocability of contracts.
The Curses of Decentralization (Chu and Wang, 2018)	Research article	Web archive	A couple of factors that inhibit smart contract scalability are identified: Disproportionality of mining power distribution, sequential programming model and incompatibility of decentralized models.
The Stakes of Smart Contracts (Verstraete, 2018)	Discussion paper	Journal	Criticism directed towards smart contract enthusiasm; code of smart contracts cannot replace traditional contract law. Moreover, smart contracts lack utilitarian efficiency and are constructed without conformity to the norms of private law.
Ethereum: State of Knowledge and research perspectives (Tikhomirov, 2017)	Conference paper	Conference / symposium	Technical overview of Ethereum transactions and structure, smart contracts and the problems with scalability, privacy, usability, programming and legal matters.
Alice in Blockchains: Surprising Security Pitfalls in PoW and PoS Blockchain Systems (Keenan, 2017)	Conference paper / solution proposal	Conference / symposium	Argues that problems with the blockchain extend deeper than just human error and span to structural defects. Elaborates possible attacks and provides possible solutions.
A Comprehensive Study on the Scalability Challenges of the Blockchain Technology (Ademi, 2018)	Bachelor thesis	Web archive	Identification of scalability/usability concerns of the blockchain, with minor remarks on smart contracts.
A survey of attacks on Ethereum smart contracts (Atzei *et al*., 2017)	Research paper	Web archive	An analysis of the security of Ethereum-based smart contracts; detection of vulnerabilities in programming through verification of smart contracts, determined by probing recent attacks.

Table 2: Continuation

Cryptocurrency and the Myth of the Trustless Transaction (Bratspies, 2018)	Discussion paper	Web archive	A critical approach to the idea of eliminating trust mechanisms. Contends the assertion that smart contracts are immutable (A hard fork allowed reversion of transfers out of the DAO).
Are Transaction Costs Drivers of Financial Institutions? Contracts Made in Heaven, Hell and the Cloud in Between (Hazard *et al.*,2016)	Research paper	Journal	Smart contracts with automation and self-enforcement would significantly decrease the costs of monitoring and enforcement in financial systems.
Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab (Delmolino *et al.*, 2016)	Solution proposal	Conference	A smart contract creation lab was formed where the pitfalls of smart contract codification were identified through mistakes that students made during the creation of smart contracts. How these mistakes can be avoided is shown.
Short Paper: Formal Verification of Smart Contracts (Bhargavan *et al.*, 2016)	Solution proposal	Conference	A framework to analyse and verify the safety and functional correctness of Solidity smart contracts using F*.
S-gram: Towards Semantic-Aware Security Auditing for Ethereum Smart Contracts (Giancaspro, 2017)	Solution proposal	Conference	Introduces S-gram, a tool that detects vulnerabilities to which statistical abnormalities are often the indicator.
Ethereum Smart Contracts: Security Vulnerabilities and Security tools (Dika, 2017)	Master thesis	Web archive	Types of security errors in smart contracts, why they occur and how they can be prevented.
Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains (Parizi *et al.*, 2018)	Research paper	Web archive	Evaluation of security testing tools that detect vulnerabilities in smart contracts written in Solidity.
Making smart contracts smarter (Luu *et al.*, 2016)	Solution proposal	Web archive	A survey of safety concerns related to Ethereum-based smart contracts. Introduction of new security problems as well as a solution to improve the system.
Vandal: A Scalable Security Analysis Framework for Smart Contracts (Brent *et al.*, 2018)	Solution proposal	Web archive	A static analysis framework for detecting susceptibilities in smart contract code is introduced.
Towards Safer Smart Contracts: A Sequence Learning Approach to Detecting Vulnerabilities (Tann *et al.*, 2018)	Solution proposal	Web archive	Proposition of a sequential learning method, which involves machine learning to create safer smart contracts, to detect security threats.

Table 2: Continuation

ZEUS: Analyzing Safety of Smart Contracts (Kalra *et al.*, 2018)	Solution proposal	Symposium	Puts forth the “ZEUS” framework to verify whether smart contracts are valid and fair.
A Concurrent Perspective on Smart Contracts (Sergey and Hobor, 2017)	Research paper	Conference	Smart contracts and concurrent objects are taken analogously; issues with concurrency are not as prominent with smart contracts. Certain notions in smart contract models do not correspond to anything in the concurrency realm under this analogy and this evokes certain speculations.
SMT-Based Verification of Solidity Smart Contracts (Alt and Reitwiessner, 2018)	Solution proposal	Journal	An empirical evaluation, using the SmartCheck tool, of errors of security tools that detect vulnerabilities in Ethereum smart contracts written in Solidity. Statistical tests are conducted.
Finding The Greedy, Prodigal and Suicidal Contracts at Scale (Nikolic *et al.*, 2018)	Solution proposal	Web archive	Introduces the “MAIAN” tool to trace vulnerabilities in Ethereum-based smart contracts. The paper categorizes vulnerabilities and presents a solution.
Towards automated generation of smart contracts (Frantz and Nowostawski, 2016)	Solution proposal	Conference	Presents the “ADICO” tool, which automatically translates human semantics into machine-readable contractual rules.
Setting standards for altering and undoing smart contracts (Marino and Juels, 2016)	Solution proposal	Symposium	Establishment of standards for changing or voiding Ethereum-based smart contracts.
Bitcoin and Crypto-currency Technologies A comprehensive introduction (Narayanan *et al.*, 2016)	Book	Book	A brief mention of vulnerabilities in Ethereum-based smart contracts: loops, the gas problem, issues with incentives, etc.

Source: authors

4. Discussion

Developments in the emerging blockchain field seek to revolutionize interaction between peers and could be of use in many different sectors, and the technology indeed promises colossal progress. Financial securities, derivatives, stocks, mortgages, ownership, supply chains, insurance, healthcare, etc., are all areas where blockchain technology is pronounced to be beneficial. A centralized network is susceptible to single-point failures; therefore, the blockchain democratized the network by distributing consensus to nodes, effectively eliminating exposure to risks of centralization. A decentralized network is not inherently problem-free; however, the mechanism only entails distributed node-specific problems. We mentioned those risks of exposure when assessing the related literature. The bulk of the studies in Table 2 shed light on an assortment of smart contract vulnerabilities, then presented solutions to either the vulnerabilities themselves or to errors within tools that detect vulnerabilities. Unanimity on what method or tool serves best is not present; furthermore, some solution proposals present their tool as a superlative to a contemporary one. Different studies point to a more nuanced version of the problem or to a different problem altogether, which can be said for the solutions themselves. This gives the impression that smart contracts are not exactly practical in application.

Another key aspect is what blockchain-based contractual agreements are set to replace. Hawlitschek *et al.* (2018) examine and rigorously present the concept of trust in shared economies from multiple perspectives. Their findings conclude that the idea of trustless systems is essentially unlikely to sustain and that a trusting mechanism must exist between peers. Chu and Wang (2018) also concur on the significance of said mechanism to ensure different forms of trust to replace decentralization. Whether it is an escrow agreement or security trading, scripting transactional operations in the current state of events is in no way a substitute to contemporary trusted-party exchange systems. Consider an example where a person purchases an object from the internet and where the money is held in a decentralized repository until you receive the object, much like in an escrow agreement. Without any trusted third party, this interaction is supposedly lower-cost, faster and safer. Taken at face value, the proposition houses certain drawbacks: code automation is not yet advanced to an extent that permits creating safe, dependable contracts, recourse is unlikely and the process is time-consuming. This entire process can be facilitated by using existing trust mechanisms, or at least requires an integrated auxiliary trust mechanism to increase the degree of reliability. It is important to note here that the blockchain itself is a trust mechanism as well, one that provides trust based on reliability to each and every practical aspect. It is abundantly clear that stability and security in the constitution of a blockchain system empower trust in that system.

Auditing is a considerable impediment. It is not only extremely difficult at the present but the real-life examples go beyond a minor predicament. The DAO contract had been scrutinized and monitored by experts, yet the perpetrators irreversibly moved $50 million away. The fact that a project so grand in scale with an expert team backing it failed to retain one third of the pool raises some concern as to the stability of the mechanism on a smaller scale. Implementing blockchain-based contractualized agreements for simpler transactions might function to the detriment of the parties. It certainly is not a plausible way to carry out transactions when there is precedent to the system failure. There are a vast number of people and organizations working on R&D to develop a safer and more secure environment for the technology; however, a concrete example is yet to be seen.

5. Conclusion

The blockchain market over the past decade, through crowdfunding and ICOs, has mustered grand sums, creating ample R&D opportunities. From supply chain management to healthcare, there are promising prospects of solutions presented to improve the overall quality of services and products in numerous areas. The search for novel blockchain areas is a trend in itself; thus, entrepreneurs seek to extrapolate the idea to different fields. As we have stated, smart contract technology is among those prospects, but at the current rate the ecosystem and the technology are not mature and call for extreme R&D efforts to render them appropriate. Trust mechanisms are not only essential parts of our system, but they cost-effectively provide adequate service with haste. Blockchain-based smart contracts currently are not an improvement to the premise and seem to be more trouble than they are worth.

References

Atzei, N., Bartoletti, M., Cimoli, T. (2017) A Survey of Attacks on Ethereum Smart Contracts (SoK), in Maffei, M., Ryan, M., eds., *Principles of Security and Trust*. POST 2017. Berlin, Heidelberg: Springer, pp. 164–186, https://doi.org/10.1007/978-3-662-54455-6_8

Bentov, I., Gabizon, A., Mizrahi, A. (2017). *Cryptocurrencies without Proof of Work*. Available at: https://arxiv.org/abs/1406.5694

Bhargavan, K., Delignat-Lavaud, A., Fournet, C. et al. (2016). Formal Verification of Smart Contracts: Short Paper. ACM Workshop on Programming Languages and Analysis for Security, Oct 2016, Vienna, Austria. Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, https://doi.org/10.1145/2993600.2993611

Chu, S., Wang, S. (2018). *The Curses of Blockchain Decentralization*. Available at: https://arxiv.org/abs/1810.02937

De Vries, A. (2018). Bitcoin's Growing Energy Problem. *Joule*, 2(5), 801–805, https://doi.org/10.1016/j.joule.2018.04.016

Delmolino, K., Arnett, M., Kosba, A. et al. (2016) Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab, in Clark, J., Meiklejohn, S., Ryan, P., Wallach, D., Brenner, M., Rohloff, K., eds., *Financial Cryptography and Data Security*. FC 2016. Berlin, Heidelberg: Springer, pp. 79–94, https://doi.org/10.1007/978-3-662-53357-4_6

Dietz, M., Moon, J., Radnai, M. (2016). *Fintechs can help incumbents, not just disrupt them*. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/fintechs-can-help-incumbents-not-just-disrupt-them

Fanning, K., Centers, D. P. (2016). Blockchain and Its Coming Impact on Financial Services. *Journal of Corporate Accounting and Finance*, *27*(5), 53–57, https://doi.org/10.1002/jcaf.22179

Frantz, Ch. K., Nowostawski, M. (2016). From Institutions to Code: Towards Automated Generation of Smart Contracts. *IEEE 1st International Workshops on Foundations and Applications of Self* Systems* (*FAS*W*), pp. 210–215, https://doi.org/10.1109/fas-w.2016.53

Gatteschi, V., Lamberti, F., Demartini, C. et al. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet*, 10(2), 20, https://doi.org/10.3390/fi10020020

Giancaspro, M. (2017). Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective. *Computer Law and Security Review*, 33(6), 825–835, https://doi.org/10.1016/j.clsr.2017.05.007

Liu, H., Liu, Ch., Zhao, W. et al. (2018). S-gram:

Towards Semantic-Aware Security Auditing for Ethereum Smart Contracts. *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*, https://doi.org/10.1145/3238147.3240728

Hawlitschek, F., Notheisen, B., Teubner, T. (2018). The Limits of Trust-free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy. *Electronic Commerce Research and Applications*, 29, 50–63, https://doi.org/10.1016/j.elerap.2018.03.005

Hertig, A. (2017). *Ethereum's Big Switch: The New Roadmap to Proof-of-Stake*. Available at: https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake

Johnson, B., Laszka, A., Grossklags, J. et al. (2014) Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools, in Böhme, R., Brenner, M., Moore, T., Smith, M., eds., *Financial Cryptography and Data Security*. FC 2014. Berlin, Heidelberg: Springer, pp. 72–86, https://doi.org/10.1007/978-3-662-44774-1_6

Luu, L., Chu, D.-H., Olickel, H. et al. (2016). Making Smart Contracts Smarter. *Proceedings of the* 2016 *ACM SIGSAC Conference on Computer and Communications Security* (*CCS* '16). ACM, New York, NY, USA, 254–269, https://doi.org/10.1145/2976749.2978309

Marino, B., Juels, A. (2016). Setting Standards for Altering and Undoing Smart Contracts, in Alferes, J., Bertossi, L., Governatori, G., Fodor, P., Roman, D., eds., *Rule Technologies. Research, Tools and Applications*. RuleML 2016. Cham: Springer, https://doi.org/10.1007/978-3-319-42019-6_10

Narayanan, A., Bonneau, J., Felten, E. et al. (2016). *Bitcoin and Cryptocurrency Technologies: a Comprehensive Introduction*. Princeton: Princeton University Press. SBN 9780691171692.

Seijas, P. L., Thompson, S., McAdams, D. (2017). *Scripting Smart Contracts for Distributed Ledger Technology*. Cryptology ePrint Archive, Report 2016/1156. Available at: http: //eprint.iacr.org/2016/1156

Siegel, D. (2016). *Understanding the DAO Attack*. Available at: https://www.coindesk.com/understanding-dao-hack-journalists

Tikhomirov, S. (2017). Ethereum: State of Knowledge and Research Perspectives. *The* 10*th International Symposium on Foundations and Practice of Security. Proceedings of the* 2018 33*rd ACM/IEEE International Conference on Automated Software Engineering* (*ASE* '18), September 3–7, 2018, Montpellier, France; New York, NY, USA: ACM, https://doi.org/10.1145/3238147