The State of the Art for Blockchain-Enabled Smart-Contract Applications in the Organization

Chibuzor Udokwu*, Aleksandr Kormiltsyn†, Kondwani Thangalimodzi‡, Alex Norta§
Department of Software Science
Tallinn University of Technology, Tallinn, Estonia
Email: *chibuzor.joseph@ttu.ee, †alexandrkormiltsyn@gmail.com, ‡kthang@ttu.ee, §alex.norta.phd@ieee.org

***Abstract*—The application and use of smart contracts in organizations require a holistic overview. This overview helps to understand the current adoption of this technology and also deduces factors that are inhibiting its use in the modern organization. This study provides a systematic review of previous studies comprising of frameworks, methods, working prototypes and simulations that demonstrate the application of smart contracts in organizations. Understanding the current state and usage of smart-contract technology in an organization is a focal point of this paper. Much progress occurs in developing technologies that support smart contracts, while little understanding exists pertaining to their usage in organizations. In this study, we identify properties of smart-contract applications in different domains of modern organizations. We further analyze and categorize challenges and problems mitigating the adoption of smart-contract applications.**

***Index Terms*—blockchain; applications; smart contract; limitations; use cases; decentralized autonomous organization**

I. Introduction

Organizations face new challenges such as information security [1], trust and transparency between different stakeholders [2], decentralization of working processes [3] and so on. The development of blockchain technology and smart contracts provides new opportunities for organizations to address these problems. Blockchain-enabled smart contracts are computer programs that are consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority [4]. Smart contracts provide organizations the possibility to collaborate and execute self-enforcing contract clauses in a blockchain network without the involvement of a third-party. While smart contracts provide new options for organizations and several studies have been carried out on how smart contracts can be applied to solve several issues affecting modern organizations, little is known about the adoption of smart contracts in organizations. This paper fills the gap by presenting an overview of the business applications supporting smart contracts. The primary research question of this paper is how to successfully adopt smart contracts in modern organizations? The answer to this question helps the reader to understand main domain problems that can be solved by smart contracts and current limitations of this technology. We deduce the following sub-questions from the primary research question. What are the domains of smart-contract applications in established organizations? The understanding of domains using smart contracts helps organizations during decision making processes about smart-contract adoption. What are the main benefits of smart-contract applications in these organization domains? Definitions of a domain help to focus on the main benefits that organizations can gain from smart-contract technology. What are the issues limiting the gains of smart contract usage in the organizations? Understanding the limitations helps to avoid serious problems while adopting smart contracts in working processes.

The remainder of the paper is structured as follows. Section I-A presents important background information. Section II provides the description of the literature-review method used in this study. Section III discusses the analysis of results. Section IV presents problem discussions and provides directions for future research. Section V concludes the results of the overview and defines limitations of the study.

A. Basic Concepts of Smart Contracts

Smart contracts are supported by blockchain technologies [5]. In this section, we summarize the concepts of blockchain technologies as follows - basic blockchain concepts and Merkle hash tree, time stamping nodes and virtual machines, consensus and solidity programming language for coding smart contracts.

Blockchain: The blockchain is a distributed ledger that allows participants to write and update records on the ledger and cryptography ensures that records stored remain the same once added [6]. Records are added to the ledger in form of transactions, and these transactions are hashed and grouped in blocks. Each block is cryptographically linked to the next block. Markel tree or hash tree is a cryptographical method that ensures transactions stored in blockchain are linked with mathematical hashes [7], [8]. This guarantees that no modification can invalidate the entire record. The hashes provide an efficient method to verify any transaction on the blockchain. With this method, records can be verified without going through the entire data stored in the network [8].

Nodes and virtual machines: The blockchain network is represented by the nodes that are connected in peers and each participating node has a copy of the ledger [6]. The nodes are

978-1-7281-1275-6/18/$31.00 ©2018 IEEE
DOI 10.1109/ISPRAS.2018.00029

run by virtual machines, e.g., an Ethereum blockchain node is powered by the Ethereum Virtual Machine (EVM) [7]. Once a new block is accepted in the network, each node updates its record by adding the new block. Transactions are timestamped and sent from the participating nodes. All the nodes in the network agree on a consensus method for adding new records to the ledger [5]. Transactions are grouped in blocks and once a block has been accepted by the network, all the participating nodes add the new block to their copy of the ledger [7].

Consensus mechanism: A consensus method is an agreed method for adding new records to the blockchain by the participating nodes. Consensus methods are grouped into two - voting based consensus and proof-based consensus [5]. Proof-of-Work (PoW) is an ex-ample of proof-based consensus method and its currently being used by the Bitcoin and the Ethereum blockchain at the time of this writing [6], [7]. PoW is a consensus mechanism that allows all the participating nodes to solve a difficult mathematical problem and rewards the first node that solves the problem by selecting the node to add the next block [5]. The Proof-of-Stake (PoS) is another example of proof-based consensus method. However, while PoW motivates a centralization of computing power, PoS moves the decision basis from computing power to possession of stake in the system, such as an amount of cryptocurrency [9].

Programming smart contracts: Solidity is an example of a programming language that provides a method for running a computer code on blockchain nodes [10]. Computer programs that digitally verify, enforce contracts and run on a blockchain network are referred to as smart contracts. The smart contracts are stored and executed in blockchain nodes. With the right access, any user can run and execute smart contract functions from any participating node in the network [7]. In our study, we focus on smart contracts written in Solidity as it is the programming language adopted by the largest blockchain network that supports smart contracts [7].

II. Method of Literature Review

This research uses a systematic literature review method [11]. Literature review gives a good foundation for research in information systems and strengthens information system as a field [12]. A review of literature of smart-contract applications strengthens the field of blockchain within information systems. We conduct the review in four phases [11]. Phase 1 is the review of the purpose and protocol of the study. Phase 2 involves searching the literature and practical screening. In Phase 3, the quality appraisal and data extraction is presented. In Phase 4, we analyze the findings. This literature review method is chosen because it is developed specifically for information-system research [11].

Planning Phase: In the first phase, we design a review protocol as this is an essential element in conducting a systematic literature-review study [13]. Furthermore, a review protocol minimizes biases in a detailed plan [13]. We discuss the purpose of the review and design a protocol, a searching plan, selection criteria, data extraction method, data analyses and present the review results.

Selection Phase: In the second phase of the review, we search for academic articles using the Google scholar database. Since smart contract is a new technology in information systems, we search for journal papers, conference papers and select white papers from 2013–2018. This time frame helps us to find relevant articles from the search engine.

In our search for articles, the keywords and Boolean operators used are as follows: smart contract + business, smart contract + organization, smart contract + organization, blockchain + business, blockchain + organization, blockchain + organization, distributed autonomous organization + business, decentralized autonomous organization + organization, to find papers with limitations and problems, the following key words are used: problem + blockchain, problem + decentralized autonomous organization, and problem + smart contracts. These pairs we use independently in every search.

From the results of our searches, we conduct an efficient screening process, discarding articles not relevant to the study, duplicates, and articles that we do not obtain the full text. After this initial screening, we got a total of 469 papers. This process is depicted in Figure 1 in the study [14].

Exclusion and Inclusion criteria: In the first step of article selection, the exclusion criteria include the following: Articles that are not relevant to the study, articles for which a full paper cannot be downloaded or accessed, articles not published between 2013 and 2018 and articles not related to blockchain technology, distributed autonomous organization, or smart contracts. In the second step, the inclusion criteria include high-quality white papers, journal papers, peer-reviewed conference papers, articles on smart-contract applications in an organization.

Execution phase: In the third phase of the review, we extract data from eligible articles based on the research questions guiding this research and collect information from articles to serve as raw material for the analyses [11].

III. Analysis of Result

In this section, we analyze the reviewed literature to understand how smart contracts are currently applied in the organizations and current limitations that mitigate the adoption of smart-contract applications in the organization. The subsections are structured as follows: Section III-A provides an analysis of smart-contract applications in the organization. Section III-B defines the blockchain issues mitigating smart-contract adoption in organizations.

A. Analyses of smart-contract applications in the organization

We base the analyses of smart-contract applications in the organizations on the following categories: the year of the publication, type of publication and subcategories to identify the properties of the smart contract. The year and type of publication provide information on the quality of the literature reviewed. We identify when the paper was published and if the paper is a peer-reviewed publication. Though there has been

too much proliferation of non-peer reviewed papers in the form of white papers in the blockchain smart-contract community, we cannot ignore so many contributions by none peer-reviewed literature in this field.

We further analyze the characteristics of the smart contract that are listed in properties categories in Table 1 in [14]. We identify the following properties of the smart contract: organization, blockchain technology, type of network, application area, problem intended to be solved and status of contribution. In the organization properties of the smart contract, we identify the type of organization that the contribution was developed for. We further divide the organizations into business and public. Under technology property, we identify the blockchain the smart contract was designed to be implemented on. With this property, we identify current blockchain technologies that support smart contracts. In the application area, we identify the type of business process/operation the smart contract is designed to simulate. In the purpose category, we identify the primary goal of applying smart contract in a particular application area, and this can be security reasons, privacy concerns, to build trust, etc. In the status section, we identify if the projects analyzed are theoretical descriptions, prototypes, or working implementations in an organization.

1) Presentation of smart-contract application analyses results: The overview of analyses of smart-contract applications in the organization is presented in the Table 1 in [14]. If a project analyzed does not address the corresponding item or provide sufficient information on the classification, we leave it unmarked. The table shows that 81% of the projects/studies analyzed are published as peer-reviewed publications. 59% of the projects are published in 2017 and 75% of all implemented projects are published from 2017 and later.

Business organizations are the top organizations for smart-contract applications as 87.5% of the projects analyzed are designed for business organization. For the projects that are implement, 75% are specifically designed for business organizations.

In all the projects analyzed, 62.5% are either prototyped, or implemented (working). Only 37.5%, fall into the category theoretical descriptions and proposed frameworks/methods.

In the application area/domain of smart-contract projects analyzed, 71.87% have their application areas in supply chain management (SCM), finance, healthcare, information security, smart city and IoT solutions. Therefore, we identify those at the top domains of smart-contract applications in the organization. Besides, for the projects that are already implemented, 75% are in the domain of healthcare, SCM, and finance. Furthermore, the table shows that transparency and trust are main reasons why an organization may use smart-contract applications, about 44% of the projects mention either transparency, or trust as the primary purpose of the smart-contract application. Other top reasons include data security/privacy, resource management, tamper proof, and interoperability.

Ethereum and Hyperledger fabric are the leading technology for smart-contract applications in organizations, as 50% of the implemented projects are hosted on these platforms. Ethereum network is the technology of choice for prototyping smart-contract projects in the organization as 66.67% of the projects analyzed are prototyped with the Ethereum network. Also, 50% of the prototypes are carried out in public blockchains. Still for implemented projects, 75% are carried out as private networks.

B. Analysis of blockchain issues mitigating smart-contract adoption

We examine existing issues and technical limitations that affect blockchain technology. Our analyses are based on the following factors: the timestamping virtual machine that runs the blockchain nodes, cryptography behind the digital signature, consensus mechanism for confirming transactions and the Solidity programming language for developing smart contract [7], [15]. We further examine how the issues identified affect different application areas of smart contracts in the organization. We only consider top application domains in this analysis.

1) Presentation of blockchain limitation analyses results: We identify 18 limitations of blockchain technologies. From the analyses as shown in Figure 2 in study [14], we found that technologies affected are a digital signature (55.6%), consensus (50%), Solidity programming language (38.9%), consensus mechanism PoW (27.8%) and nodes (27.8%).

We analyze application areas that are affected by presented limitations. Most of the limitations (61.1%) describe issues that affect all application areas that we investigate. 72.2% of the limitations define the issues that affect all applications that use tokens. Limitations that affect an application involving PoW are presented in 66.7% and applications in public blockchains are presented each by 72.2%. Limitations for applications in finance domain are presented in (72.2%) and 66.7% describes limitations that affect IoT, Smart City and SCM domains.

Figure 3 in the study [14], shows how the current limitations of blockchains affect smart contracts in public networks and private networks. The figure shows that there are specific issues in blockchains that affect only the public networks. However, most limitations affect both private and public blockchains. No specific issue affects only private blockchains. The issue of unsustainable consensus method presented in PoW does not affect private blockchains, because they mostly use voting-based consensus method for approving transactions [16]. Due to the control that exists in permissioned blockchains when approving members, the trusted-party-requirement issue is eliminated since all participating nodes are known and trusted.

We further analyze Table 2 in [14] to determine the severities of the current limitations that affect blockchains. With this, we identify important issues mitigating smart contracts usage in the organization. The classification for this analysis is based on the following severity levels: low important, significant and critical.

Figure 4 in the study [14] shows the severity levels of the current issues that affect blockchain technologies. The issues

are ordered in their level of importance. The less important issues are in at the bottom of the triangle, significant issues are in the mid-level of the triangle while the critical issues are located at the top of the triangle. The study [14] identifies the following main limitations of blockchains technologies: usability and complexity issues, standardization, lack of testing and practical experience, and design architecture issues. Other significant issues include storage scalability, regulation, soundness of smart contracts, security flaws and bugs, privacy leakage and smart contract lifecycle management and non-tested consensus methods. The less important issues are as follows anonymity, scalability-time, transaction cost, cryptocurrency unpredictability, unsustainable consensus method, trusted third-party involvement and cryptocurrency liquidity problem.

IV. Discussions

In this section, we discuss the results of the analyses we performed in section III. The results of the analyses are presented in Table 1 and 2 of the study [14]. In the first part of this section, we discuss the results of the analyses showing smart-contract applications in the organization. In the second part of this section, we discuss the current blockchain technology issues that affect smart contracts usage in the organization.

A. Application discussion

The results from the Table 1 in study III show that most are mostly peer-reviewed academic publications. This is a necessary step in determining the quality of the projects we evaluate in our study. Though the idea of smart contracts begins with the unpublished manuscript by Szabo Nick in 1994[1] and the implementation starts with the development of the Ethereum virtual machine that provides the possibility of running Turing complete programs on a blockchain in 2014 [7], our study shows that serious effort to develop organization-blockchain applications start in 2017. This is evident as most of the implemented smart-contract projects are carried out in 2017 and later. Blockchain provides an opportunity for both public- and private organizations to run trustless smart-contract applications. The current study shows that business organizations lead in development, implementation, and adoption of smart-contract projects. Our study did not identify any specific smart-contract project designed for military organizations. A search on Google Scholar for "military blockchain applications" returns about 1200 results. However, our study cannot identify an actual prototype, or working blockchain based military organization application. This could be linked to the fact that military applications are usually classified and not available in public domains.

In our study, we identify top application areas, or organization domains that comprise a large number of smart-contract projects. We identify the following organization domains as the top application areas of smart contracts - SCM, finance, healthcare, information security, smart city and IoT solutions. These organization domains have some similarities because their processes involve the participation of several collaborating parties. For instance, SCM involves parties from a supplier, buyer, transporter, etc., who do not trust each other. Blockchain enabled smart contracts therefore are very relevant in these domains as they provide a trustless and transparent system for storing and executing transactions in an immutable way. To validate this point, our study also shows that trust and transparency are the top reasons to adopt blockchains for all the projects we evaluate.

Though there are many blockchains for executing smart contracts, our study shows that Ethereum blockchain remains the blockchain of choice for prototyping smart-contract projects. Still, projects are developed using Ethereum and Hyperledger fabric blockchains. Hyperledger fabric is part of the blockchain tools developed in the open source Hyperledger project. The Hyperledger project seeks to develop compatible and interoperable blockchain frameworks across organizations. IBM is a leading contributor to the Hyperledger fabric project, and also a leading service provider for organizations adopting blockchain projects [17]. Finally, our study shows that most of the working projects are implemented on permissioned networks. This is because of the privacy leakage blockchain issue that causes transactions to be viewable to all participants of the network. Even though the privacy leakage problem affects both private- and public networks, as shown in our study, this problem is reduced in private blockchains because permissioned networks can regulate the membership and participation in their network.

B. Discussion of Limitations

In this section, we discuss current limitations affecting blockchain technologies. In the second part of the section, we discuss current research addressing important limitations that mitigate the adoption of smart contracts.

1) Smart contract and blockchain limitations: Both public- and private blockchain networks face challenges regarding to who is allowed to take part in the network, who is allowed to execute the consensus protocol, and who is responsible for maintenance of the shared ledger [18]. The usage of smart-contract applications in organizations is complicated because of the blockchain complexity- and usability issues. Blockchain networks have complexity and usability challenges, especially for first-time users [19]. Furthermore, the blockchain technology has architecture-design issues that are not acceptable for organization processes [17]. Smart contracts are supported by a few number of programming languages such as Solidity, Cardano, Tezos, Neo etc. The consensus mechanisms are not flexible and are hardcoded into the blockchain [17].

Several limitations affect blockchain-technology consensus mechanisms. Cost is attached to performing transactions in the blockchain to compensate miners, and this may limit the usage of smart contracts in organization applications. Still, this does not apply to private blockchain networks as voting-based consensus methods are usually adopted in permissioned

[1]Szabo, Nick. "Smart contracts." Unpublished manuscript (1994).

blockchains [5], [17]. The other limitation of the blockchain consensus mechanism is volatility of cryptocurrencies and presents difficulty in making long-term economic decisions [20].

Some of the newly proposed consensus methods lack testing and reliability, similar to the well-known PoW and PoS [5]. The mechanism of a digital signature in the blockchain has several limitations. These include anonymity issues, privacy leakage in transactions and trusted third-party involvement [6], [21]. The usage of smart-contract applications that generate a significant amount of data, is limited by the storage scalability issue of blockchain nodes [21]. This affects smart-contract applications that process and store a significant amount of data.

Some of the newly proposed consensus methods lack testing and reliability, similar to the well-known PoW and PoS [5]. The mechanism of a digital signature in the blockchain has several limitations. These include anonymity issues, privacy leakage in transactions and trusted third-party involvement [6], [21]. The usage of smart-contract applications that generate a significant amount of data, is limited by the storage scalability issue of blockchain nodes [21]. This affects smart-contract applications that process and store a significant amount of data.

The Solidity programming language has several design issues such as security flaws and bugs, soundness and lifecycle management. There are many unknown attack vectors in the ecosystem and there is also the issue of bugs in Solidity code [22]. Additionally, Solidity lacks a formal foundation and smart contract cannot be verified with an algorithmic tool before they are deployed [22]. Another big challenge affecting both public- and private blockchains is the regulation of the network. There is no proper legal framework to address legal issues of tokens, tax and intellectual property in a blockchain network [23], [24].

2) Current research efforts that address significant and critical blockchain limitations: Some of the issues limiting smart-contract adoption have already been addressed. For instance, the PoS consensus method is designed to address the time scalability issue and resource wastage issue in PoW. In PoS, a consensus is achieved by randomly selecting one of the nodes to create the next block based on their stake in the network. The chances to be chosen depends on wealth in the system [25]. As a result, some of the prominent blockchain platforms such as Ethereum are adopting PoS as a consensus method for their blockchains [26]. Qtum which is also a popular blockchain platform, comprises a PoS-consensus method since inception [27].

3) Scalability, third-party involvement and privacy leakage: The issue of storage scalability is a significant limitation of smart-contract applications, as shown in our study. A study [28] proposes using decentralized database storage systems that are linked to an existing blockchain network for storing large sets of data from smart-contract applications. In these systems, immutability and trust can be achieved by applying voting mechanisms and shared replications of stored data. The main drawback of this proposal is that the storage is located outside a blockchain network and the immutability feature that blockchain provides cannot be guaranteed in these systems.

In the case of a third-party involvement, some smart-contract applications require a third party to provide information on the status, or value of an asset. IBM develops microcomputers to address this issue. These computers are so small that they can be attached directly to an asset and provide an update on the asset[2] . This is particularly useful in the SCM domain. The current setup of smart-contract applications in the SCM domain requires an RFID chip, or similar tool to provide information on the status of assets [3], [29]. We consider this a third-party involvement because the information is not directly provided by a blockchain node. With the microcomputers that can be attached to an asset, the asset itself turns into a blockchain node, providing information on its status without the involvement of a third party.

Other research addresses the issue of information confidentiality in blockchains. The design of blockchain enables all participants of a network to view the transactions in the network. Some studies [30], [31] propose the use of private blockchain networks to address this issue. Though participation in private blockchain networks can be regulated, privacy leakage is still an issue, even in permissioned networks. Business processes require that only certain members of an organization have access. Therefore, privacy leakage is still an issue because there is currently no method to control access to information on blockchain networks. Still, study [32] addresses this issue proposing a cryptographical protocol called HAWK that ensures the privacy of data stored in a public blockchain. This is achieved by adding an additional compiler to transform standard smart contracts to a cryptographical protocol among the users of a blockchain. To achieve confidentiality, the public key of a trusted third-party node is used to encrypt and decrypt information among the parties involved in the contract. The use of a trusted third party is a significant drawback of this protocol as this violates the decentralization and transparency principles of a blockchain. There is also an issue of additional cost for verifying the transactions performed using this protocol [32].

4) Testing, design and usability issues: One of the testing issues identified in our study is a lack of proper testing frameworks for blockchain applications. As a recent technology, blockchain applications have not been properly tested and may fail at some point. There are currently no fault injection frameworks available for testing blockchain implementations. Available techniques do not cover Byzantine failures as represented in blockchain applications [33]. The study [33] proposes a new generation of fault injection frameworks for deployment in production to challenge blockchain-based distributed systems. The study proposes using the framework to perturb and verify permissioned blockchain technologies with Byzantine failures. As there is not much practical experience in usage of such projects, blockchain implementations cannot be tested

[2]IBM's New 'World's Smallest Computer' Is Built For Blockchain http://bitcoinist.com/ibms-new-worlds-smallest-computer-built-blockchain/ (accessed May 2018)

appropriately. As a result, organizations do not quickly move their business processes to blockchain solutions.

Blockchain technology is new and therefore, there are unknown attack vectors in the blockchain ecosystems. The Solidity programming language has known security bugs. When used as a payout address, a smart contract acquires the control of a sender's contract and withdraw funds from it [34].

Non-flexible consensus methods limit the usage of specific platforms and thus, not all business requirements can be implemented in such an environment. Organizations should be able to decide what consensus method is most suitable for their applications. To solve this problem, the Hyperledger Fabric platform provides the possibility for smart contract developers to choose the most suitable consensus method for their projects before deploying with a blockchain [17]. Still, the main limitation is that PoS and PoW as the most popular consensus methods, are not available for the Hyperledger platform.

5) Regulation, standardization and smart contract lifecycle management: The development of blockchain standards and regulations is at an early stage [35]. Blockchain is a new technology and therefore it is too early to determine the regulations required [36]. Little research exists about standardization and regulation. Still, standards development is underway to address the risks and abuses. On the other hand, it is essential to avoid overregulation that stifles innovation because establishing laws will have an impact on blockchain technology development [35], [37]. Different blockchain platforms currently exist that are not interoperable, developing blockchain standards are necessary in ensuring interoperability between multiple blockchain implementations, stronger consensus, security and resilience, privacy and trust [38].

Although smart contract lifecycle management is identified in this study as part of the issues mitigating smart-contract adoption in the organization, significant research efforts have been made in addressing this issue. The study [16], proposes a method for managing web-based electronic contract. Although, the study focuses on electronic contracts that are run from web systems instead of blockchain systems as used in smart contracts, we consider the study useful because the latter is a form of electronic contract deployed in a blockchain network. Therefore, the same management cycle is applicable to both smart contracts and other forms of electronic contracts. The study proposes a six-step approach to manage smart contracts comprising proposal, configuration, publication, negotiation, operation, and closure. Thus, the design of a specific contract/agreement holds for a single business operation and once the goal of the operation is achieved and all parties are satisfied, the contract is closed and a new one created. The major drawbacks are that smart contracts are designed for business processes with rules that do not change quickly since modifications, or changes, cannot be performed on smart contracts once they are deployed on a blockchain [7]. Further studies must be carried out to provide an appropriate method for managing the lifecycle of a smart contract.

The study [39] provides a formalized lifecycle management framework for decentralized applications. The study describes a four-phase steps in managing smart-contracts and they as follows – setup phase, description of decentralized governance infrastructure (DGI), enactment phase and termination phase. The setup phase describes the contract negotiation stage as the parties involves describes the services required and agree on a proposal for the contract. The DGI shows in hierarchical order the elements required in executing electronic transaction in the contract proposal. Enactment phase shows the implementation and the behavior monitoring of the contract on DGI. Finally, termination phase shows steps required in dissolving the contract. The framework also provides the possibility for transaction rollback when there is conflict as well as compensation mechanisms in such cases.

6) Blockchain cloud platforms: Blockchain as a Service (BaaS) is a new cloud computing service offered to organizations for processing their business operations via blockchain networks [40], [41]. IBM[3], Microsoft[4] and SAP[5] are leading providers of blockchain-cloud service, while other cloud providers are also integrating existing blockchain platforms as part of service offerings[6]. For instance, Amazon recently adopted QTUM as part of the blockchain platforms for its web service offerings . Different methods are proposed for implementing blockchain cloud service. The study [40] proposes a functional blockchain as a service concept that offers a lighter implementation of top-level business logic applicable in BaaS. The main advantage of this approach is reducing the complexity of developing business logic over blockchain to improve performance.

Although BaaS reduces the complexities for organizations wishing to adopt blockchain for their business process, cloud-blockchain based services still experiences some blockchain limitations that are outlined in this study. Storage oversize is the main limitation of blockchain-based cloud platforms [40]. There is also an issue of third-party involvement that negates the main principles of blockchain.

V. Conclusion

In this paper, we analyze 48 peer-reviewed papers relevant to our research question how to successfully adopt smart contracts in modern organizations? These papers are filtered out from the initial search results of 496 papers. Then we categorize the selected papers by year, type of organization, blockchain technology, type of network, application area, problem intended to be solved and status of contribution. Finally, we examine existing issues and technical limitation of blockchain technology affected.

Our analysis shows that most of the organizations that adopt smart-contract application are private (87.5%). 75% of already implemented projects are designed specifically for private

[3]IBM Blockchain: https://www.ibm.com/blockchain

[4]Microsoft Azure platform: https://azure.microsoft.com/en-us/solutions/blockchain/

[5]SAP Blockchain service: https://www.sap.com/products/leonardo/blockchain.html

[6]Amazon blockchain: https://aws.amazon.com/marketplace/seller-profile?id=884fa2fc-5050-4db4-9110-c9a616d10e99

organizations. Most of the analyzed projects (62.5%) are either prototyped or implemented. Only 37.5% fall under theoretical descriptions and proposed frameworks/methods. Top domains (71.87%) of organizations adopting smart-contract applications are aupply chain management (SCM), finance, healthcare, information security, smart city and IoT solutions. The implemented projects are mostly (75%) presented in healthcare, SCM and finance domains.

After analyzing the organizations adopting smart contracts we check the purposes of doing so. According to our research, the transparency and trust are the main benefits with 44% of smart contracts used in organizations. Other benefits include data security and privacy, resource management, tamper-proof, and interoperability.

We identify 18 limitations of blockchain technologies. The technologies affected are a digital signature (55.6%), consensus (50%), Solidity programming language (38.9%), consensus mechanism PoW (27.8%) and nodes (27.8%). Most of the limitations (61.1%) describe issues that affect all investigated application areas. 72.2% of the limitations define the issues that affect all applications that use tokens. 66.7% of the limitations affect applications involving PoW, applications in public blockchains are presented each by 72.2%. Limitations for applications in the finance domain are presented in 72.2% and 66.7% describe limitations that affect IoT, smart city and SCM domains.

Our study has some limitations, and these include the scope of analyzed projects and an inadequate categorization of decentralized applications to consider viable projects. Our study considers only projects that are in academic publications while there are other smart-contract projects in organizations that are not presented in any academic publication. As future work, we propose a study to evaluate the feasibility and usability of implemented decentralized applications in the blockchain ecosystem.

REFERENCES

[1] S. Shah, "Use of blockchain as a software component to send messages anonymously for a data trading platform," 2017.

[2] C. Stagnaro, "White paper: Innovative blockchain uses in health care," *Freed Associates*, 2017.

[3] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," 2016.

[4] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: platforms, applications, and design patterns," in *International Conference on Financial Cryptography and Data Security*. Springer, 2017, pp. 494–509.

[5] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain." *Journal of Information Processing Systems*, vol. 14, no. 1, 2018.

[6] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[7] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, 2014.

[8] G. Becker, "Merkle signature schemes, merkle trees and their cryptanalysis," *Ruhr-University Bochum, Tech. Rep*, 2008.

[9] Z. Liu, S. Tang, S. S. Chow, Z. Liu, Y. Long, and Z. Sui, "Fork-free hybrid consensus with flexible proof-of-activity," Cryptology ePrint Archive, Report 2017/367, Tech. Rep., 2017.

[10] C. Dannen, *Introducing Ethereum and Solidity*. Springer, 2017.

[11] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," 2010.

[12] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS quarterly*, pp. xiii–xxiii, 2002.

[13] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of systems and software*, vol. 80, no. 4, pp. 571–583, 2007.

[14] C. Udokwu, A. Kormiltsyn, K. Thangalimodzi, and A. Norta, "An exploration of blockchain enabled smart-contracts application in the enterprise," Technical Report, DOI: 10.13140/RG.2.2.36464.97287, Tech. Rep.

[15] J. Sidhu, "Syscoin: A peer-to-peer electronic cash system with blockchain-based services for e-business," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*. IEEE, 2017, pp. 1–6.

[16] J. B. Neto and C. M. Hirata, "Lifecycle for management of e-contracts based on web service," in *Proceedings of the World Congress on Engineering and Computer Science*, vol. 1, 2013.

[17] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018, p. 30.

[18] P. Jayachandran, "The difference between public and private blockchain," *IBM Blockchain Blog, May*, vol. 31, 2017.

[19] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[20] G. C. Dumitrescu, "Bitcoin–a brief analysis of the advantages and disadvantages," *Global Economic Observer*, vol. 5, no. 2, pp. 63–71, 2017.

[21] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Work Pap.–2016*, 2016.

[22] S. Eskandari, J. Clark, V. Sundaresan, and M. Adham, "On the feasibility of decentralized derivatives markets," in *International Conference on Financial Cryptography and Data Security*. Springer, 2017, pp. 553–567.

[23] M. Fenwick, W. A. Kaal, and E. P. Vermeulen, "Legal education in the blockchain revolution," *Vand. J. Ent. & Tech. L.*, vol. 20, p. 351, 2017.

[24] B. Notheisen, M. Gödde, and C. Weinhardt, "Trading stocks on blocks-engineering decentralized markets," in *International Conference on Design Science Research in Information Systems*. Springer, 2017, pp. 474–478.

[25] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[26] P. Dai, N. Mahi, J. Earls, and A. Norta, "Smart-contract value-transfer protocols on a distributed mobile application platform," *URL: https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3. pdf*, 2017.

[27] T. Bocek and B. Stiller, "Smart contracts–blockchains in the wings," in *Digital Marketplaces Unleashed*. Springer, 2018, pp. 169–184.

[28] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, "Bigchaindb: a scalable blockchain database," *white paper, BigChainDB*, 2016.

[29] E. Hofmann and M. Rüsch, "Industry 4.0 and the current status as well as future prospects on logistics," *Computers in Industry*, vol. 89, pp. 23–34, 2017.

[30] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*. ACM, 2016, pp. 29–36.

[31] M. Vukolić, "Rethinking permissioned blockchains," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 2017, pp. 3–7.

[32] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[33] M. A. González, W. Rudametkin, M. Monperrus, and R. Rouvoy, "Challenging anti-fragile blockchain applications," in *11th EuroSys Doctoral Workshop EuroDW'17*, 2017.

[34] M. Knecht and B. Stiller, "Smartdemap: A smart contract deployment and management platform," in *IFIP International Conference on Autonomous Infrastructure, Management and Security*. Springer, 2017, pp. 159–164.

[35] D. He, K. F. Habermeier, R. B. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura, T. S. Sedik, N. Stetsenko *et al.*, "Virtual currencies and beyond: initial considerations," International Monetary Fund, Tech. Rep., 2016.
[36] D. Blummont, "Blocking the future? the regulation of distributed ledgers," 2017.
[37] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, 2017.
[38] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, "Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards," *Overview report The British Standards Institution (BSI)*, 2017.
[39] A. Norta, A. B. Othman, and K. Taveter, "Conflict-resolution lifecycles for governed decentralized autonomous organization collaboration," in *Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*. ACM, 2015, pp. 244–257.
[40] H. Chen and L.-J. Zhang, "Fbaas: Functional blockchain as a service," in *International Conference on Blockchain*. Springer, 2018, pp. 243–250.
[41] J. Singh and J. D. Michels, "Blockchain as a service: Providers and trust," 2017.