2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing,
Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics

Blockchain Use Cases in Digital Sectors: A Review of the Literature

Shiroq Al-Megren*, Shada Alsalamah*†, Lina Altoaimy*, Hessah Alsalamah*, Leili Soltanisehat‡,
Emad Almutairi§, and Alex ‘Sandy’ Pentland†

* *College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia.*
Emails: {salmegren, saalsalamah, ltoaimy, halsalamah}@ksu.edu.sa
† *Media Lab, Massachusetts Institute of Technology, Cambridge, MA 02139, USA.*
Emails: {shada, sandy}@media.mit.edu
‡ *Department of Engineering Management and Systems Engineering, Old Dominion University, Norflok, VA, USA.*
Email: lsolt001@odu.edu
§ *National Center for Cybersecurity Technologies, King Abdulaziz City of Science and Technology, Riyadh, Saudi Arabia.*
Email: ealmutairi@kacst.edu.sa

***Abstract*—Blockchain technology is a ledger system that is popularly known as the backbone of the Bitcoin cryptocurrency. Since its conception, the potential beneficial applications of blockchain in other digital sectors have been lauded in the literature, and related challenges have been disputed. In this study, the literature is reviewed for frameworks and use cases that fully realize the applicability of blockchain beyond financial applications and cryptocurrencies. A network analysis of the literature was performed to identify the most popularly documented digital sectors in this context, which include the Internet of Things (IoT), healthcare, supply chain management, and government sectors. For each sector, this review documents use cases in which an attempt is made to implement blockchain solutions. The main purpose of this paper is to probe each sector for the growing maturity of blockchain technology and to document the unique benefits and challenges arising from the use of this technology. The findings show that despite the growing reputation of blockchain technology, its implementation within these four sectors remains in infancy because the use cases lack concrete evaluations of its effectiveness and plausibility. Nevertheless, the categorization of current blockchain use cases demonstrates current applications and sector-specific concerns that suggest future directions for further research.**

***Index Terms*—Blockchain; review; network analysis; healthcare; government; Internet of Things (IoT); supply chain.**

1. Introduction

The blockchain is a ledger system that is popularly known as the underlying technology of the Bitcoin cryptocurrency that makes it possible to maintain the integrity of transaction data [1]. The technology’s ledger is decentralized and distributed, with transactions, agreements, and controls stored in digital records. In 2015, The Financial Times [2] stated that “*At its core, blockchain is a network of computers, all of which must approve a transaction has taken place before it is recorded, in a ‘chain’ of computer code. [...] The details of the transfer are recorded on a public ledger that anyone on the network can see*” [2].

Since the conception of Bitcoin, several improvements have been proposed to overcome some of blockchain’s weaknesses [3], e.g., scalability and lack of anonymity . The underlying features of blockchain technology lend themselves to financial services. In particular, blockchain technology distributes the control of the registration of transactions, the verification of identity, and the finalization of contracts, which are financial services that are traditionally centralized and managed by a third-party organization [4].

Numerous studies have also investigated the application of blockchain technology in multitudinous digital sectors that go beyond financial services. This increased interest spans several diverse fields, including corporate, governmental, and cross-industry applications. Blockchain technology has the potential to invigorate established corporate operations, such as those in healthcare and supply chain management, to overcome issues relating to security, privacy, and shareability by maintaining a common database of information. Blockchain initiatives for new-generation information infrastructures in the government domain have been undertaken by several digital champion countries, including the United Kingdom, the United States, Estonia, New Zealand, and Israel [5]. Cross-industry interest in blockchain solutions is similarly blooming due to the technology’s attractive capabilities of maintaining a distributed immutable ledger and thus creating a secure network among untrusted users.

There have been several surveys of blockchain technology that have acknowledged its growth and progression as a technical paradigm. General overviews of the advancement of blockchain have been conducted to gauge current research topics, challenges, and future directions from a technical perspective (e.g., [6], [7], [8], [9]). These reviews were often systematic, and their findings revealed the main focus of blockchain research. The potential of blockchain has also been reviewed in the literature for numerous domains and

978-1-5386-7975-3/18/$31.00 ©2018 IEEE
DOI 10.1109/Cybermatics_2018.2018.00242

contexts, including smart devices and distributed renewable energy grids [10], the Internet of Things (IoT) [11], [12], big data [13], business organization [14], and government information services [5].

In contrast to the reviews mentioned above, this paper explores the progression of blockchain utilization by its most common advocates. The review first identifies relevant digital sectors beyond financial applications and cryptocurrencies via a network analysis of the literature, the findings of which highlight the IoT, healthcare, supply chain management, and government sectors as the application domains related to the most commonly used keywords. The goal of this review is to analyze, for each application sector, the means of utilizing blockchain technology and its reported impact within the thematic context, thereby addressing the maturity of blockchain growth within the various sectors.

The remainder of this paper is organized as follows. Section 2 presents background information on blockchain technology. Next, the review design and methodology are described in section 3. An overview of the findings across the four identified digital sectors is presented in section 4. Sections 5 to 8 present overviews of the four digital sectors dominating the applications of blockchain technology outside of the financial sector: IoT, healthcare, supply chain management, and government. Section 9 follows with a discussion of the research questions and findings across sectors. Finally, section 10 summarizes and concludes the paper.

2. Blockchain Fundamentals

The blockchain is a shared ledger distributed over decentralized network nodes and holding transaction data [15]. It enables peer-to-peer communication between parties without the need for an intermediary, and it offers transparency and trust between parties [15], [16]. Blockchain technology first appeared in the Bitcoin ecosystem launched by Nakamoto in 2008, in which it underlies the Bitcoin digital payment system [1]. The blockchain can be divided into three main components: a decentralized network, shared records (ledger), and digital transactions. The technology is decentralized since it is a peer-to-peer network in which participating nodes exchange properties without the need for an intermediary. Network participants are able to view the entire shared ledger and add new digital transactions under certain access control conditions. Digital transactions in the blockchain can be stored as various types of data depending on the context and needs of the application [16].

Blockchain is a chain of blocks linked in a series, where each block points to the previous (parent) block by including the previous block's hash in its header. The process of adding a new block to the blockchain involves several steps. The sender first creates the transaction block and digitally signs it. Then, the new block is broadcast to the network participants. The new block will be added to the blockchain as soon as the majority of the participants agree on its validity. The validation of a new block involves a consensus mechanism (i.e. mining) to ensure the consistency of the distributed ledger throughout the network; for example, proof-of-work consensus is utilized for Bitcoin [17].

For blockchain technology to be utilized in various digital sectors, its original features need to be altered. One of the main modifications (in developed versions 2.0 to 4.0) is to incorporate access control into the blockchain by means of unique identifiers such that all participants are known [15]. Additionally, unlike in Bitcoin, a blockchain can have a consortium structure (only predefined nodes can mine) or a private structure (mining is performed by a single node) [4]. The shared ledger and the consensus model are some of the main concepts underlying recent blockchain applications in sectors beyond cryptocurrencies.

2.1. Blockchain Benefits and Challenges

Benefits. Blockchain is a disintermediation technology, since it avoids the effort required for controlling transactions by eliminating third-party control. In addition, blockchain's decentralization of its shared ledger eliminates the threat of a single point of failure and traffic congestion. The technology also guarantees persistence, since it is computationally impossible to delete or alter any transaction blocks once they have been recorded in the ledger. A consensus property is also achieved since the majority of miners must validate a block prior to its insertion into the blockchain. Furthermore, blockchain technology provides finality, since there is only a single distributed ledger that serves as a trusted reference for block verification [15]. Auditability is also facilitated by the technology because each block maintains a reference to its parent block and a timestamp.

Blockchain technology is presumed to have multiple beneficial security properties. Integrity is achieved through the fact that each transaction block must be digitally signed with the owner's private key and assigned a hash. Moreover, the ledger is persistent, making it immutable and tamper-resistant, which, in turn, ensures integrity. A security benefit of blockchain technology is that each network user maintains a unique pair of keys (public and private) that are used to sign and verify transaction blocks. As a result, authenticity is achieved even in public structures. For the same reason, a non-repudiation security property emerges since participants cannot deny adding a block to the ledger.

Challenges. Despite the aforementioned benefits, blockchain technology also faces several challenges in implementation. One of the most significant challenges relates to the scalability of the blockchain. In a blockchain network, the entire ledger (consisting of millions of transaction blocks) is stored in each network node. This raises the issue of storage limitations at the nodes. Another drawback pertains to the fact that due to the consensus process, the throughput rate (for transaction validation) is relatively low, and the latency is relatively high compared with a conventional system. With a consensus mechanism such as the proof-of-work mechanism, the majority of network nodes must validate a transaction block for insertion into the ledger. Additionally, there is likely to be an enormous number of transaction blocks that require validation at the same time. For instance, the Bitcoin network can perform only seven transactions per second. In fact, on average, it requires up to 10 minutes for each transaction to be validated and recorded. The mining process in a blockchain requires a considerable amount of computation that consumes large amounts of energy, which could arguably be regarded as a waste of resources [15]. A final downside of blockchain technology is that it does not guarantee confidentiality since the block content is not encrypted and all nodes share the ledger, in which all records are stored in plain text. This, of course, introduces privacy issues, particularly in the case of public ledgers.

3. Review Design

The goal of this research is to provide an overview of fully realized and documented blockchain use cases in order to identify themes beyond cryptocurrencies and financial services. Thus, it is shown that the underlying ideas behind blockchain technology, namely, a public ledger and a decentralized environment, are applicable in numerous environments. Nevertheless, this review considers only research that examines the particularities and challenges of the application of blockchain solutions.

3.1. Research Questions

To achieve the review's goal, the following research questions (RQs) were formulated:

RQ1: What are the environments of blockchain application beyond cryptocurrencies and financial services? The main research question aims to identify applications of blockchain technology that go beyond cryptocurrencies and financial services. This question highlights the main environments in which blockchain has been utilized as a solution.

RQ2: What is the blockchain structure used within each environment? The purpose of this question is to identify the building blocks of the blockchain technology when utilized within a given environment. These include the type of blockchain, the type of data stored in the blockchain, and the data storage and mining techniques.

RQ3: What are the potential advantages of blockchain adoption in each environment? The potential benefits of the utilization of blockchain technology have been widely discussed in the literature. With this question, the review highlights the direct benefits that stem from a given environment's needs and blockchain's advantages.

RQ4: What are the challenges associated with the adoption of blockchain in each environment? This question serves as a counterpoint to RQ3, with the purpose of identifying the unique challenges of blockchain technology in the context of each of the identified environments.

3.2. Search Technique

An analysis of the Web of Science literature was conducted using the NAILS tool [18]. NAILS performs statistical and social network analyses on citation data to identify important authors, journals, and keywords in the dataset based on occurrences and citation counts. The analyzed dataset consisted of 411 publication, and each was associated with 74 variables that were processed by the tool. The keyword results were further analyzed to identify the main environments of blockchain application (see section 4). These results were then used to formulate the search string for each of the identified environments. Each search string consisted of two main components: the term 'blockchain' and the application environment discovered via the literature analysis. The main electronic database sources into which each search string was fed in order to search for use cases were IEEE Xplore, Web of Science, and Google Scholar. To identify which papers to examine, an exclusion stage was performed to eliminate papers that addressed the application of blockchain technology only theoretically, without considering implementation.

4. Findings

The results regarding RQ1 were extracted from the analysis of the Web of Science literature. Important keywords were identified and sorted by the number of articles in which each keyword was mentioned and by the total number of citations for each keyword. Understandably, the term 'blockchain' was the most frequently mentioned and cited among the keywords, followed by 'Bitcoin' and 'smart contracts'. 'Internet of Things' followed next in the list of most cited keywords, being repeatedly mentioned in the literature. 'Healthcare' and 'electronic medical records' were found to have been used as keywords in various articles and similarly received a considerable number of citations. The term 'supply chain' was mentioned several times in the literature, while the term 'distributed system' was more frequently cited. Terms related to the government sector, such as 'government', 'smart government', and 'e-government', were the least frequently addressed in the literature.

The answer to RQ2 is presented in detail in sections 5, 6, 7, and 8 for each of the environments identified. The benefits (RQ3) and challenges (RQ4) of blockchain adoption within the context of each of the environments identified are summarized in Tables 1 and 2, respectively. The results are further discussed in the following sections for each of the selected environments.

5. Internet of Things

IoT can be described as a collection of connected devices and sensors that have the ability to sense and gather data from their surrounding environment. Within an IoT environment, the sensors are typically small and limited in resources, and the network demands low latency and has limited bandwidth. In addition, an IoT network can connect millions of devices with various storage and computational capabilities. Due to this heterogeneous nature of the data and resources, IoT is vulnerable to a number of privacy and security issues. Blockchain technology is a promising

Benefit	IoT	Healthcare	Supply Chain	Government
Accountability		✓		✓
Adaptability		✓	✓	✓
Anonymity	✓		✓	
Auditability	✓	✓	✓	✓
Availability	✓	✓		✓
Credibility		✓		✓
Confidentiality	✓	✓	✓	✓
Decentralization	✓	✓	✓	✓
Immutability	✓	✓	✓	✓
Integrity	✓	✓	✓	✓
Provenance		✓	✓	✓
Transparency	✓	✓	✓	✓
Trust		✓	✓	✓

TABLE 1. THE BENEFITS OF BLOCKCHAIN TECHNOLOGY ADOPTION WITHIN THE DIGITAL SECTORS/ENVIRONMENTS.

Challenge	IoT	Healthcare	Supply Chain	Government
Computational overhead	✓	✓	✓	✓
Interoperability		✓	✓	
Latency	✓			
Privacy		✓	✓	
Scalability	✓			
Storage	✓	✓	✓	✓

TABLE 2. THE CHALLENGES OF ADOPTING BLOCKCHAIN TECHNOLOGY WITHIN THE DIGITAL SECTORS/ENVIRONMENTS.

solution for a verifiable, secure, and immutable method of recording data obtained through IoT techniques.

A blockchain infrastructure has been utilized to provide software update availability and innocuousness for IoT devices from different manufacturers [19]. The proposed solution consists of three components: a web portal, a blockchain infrastructure, and several devices. Device manufacturers deploy software updates via the web portal. These updates are pushed into the blockchain to store. Meanwhile, IoT devices periodically check for updates from the blockchain. Once an update becomes available, a device downloads and installs the update and then sends an acknowledgment to the blockchain infrastructure. The utilization of blockchain technology for software updates can dramatically improve their availability to IoT nodes due to block immutability and persistence while also mitigating risks.

A lightweight architecture for IoT that utilizes Bitcoin's underlying blockchain technology has been proposed to overcome challenges related to computational overhead and latency [20]. A proof-of-concept IoT system was presented as an example, which consists of three components: a smart home, an overlay network, and cloud storage. It eliminates the original resource-consuming Bitcoin mining strategy and the concept of coins. The devices are centrally managed by a home miner, i.e., a device for monitoring transactions. A blockchain is utilized to maintain the transactions, which are governed by a policy header. Transactions vary to enable data storage, access, and monitoring to ensure security. The effectiveness of this concept against security attacks was analyzed. The results demonstrate that the proposed architecture incurs a lower computational overhead while achieving significant security and privacy advantages.

FairAccess is an access control framework for IoT that is based on blockchain technology [21]. In FairAccess, the blockchain is used as a database for storing all access control policies and for logging users' transactions to ensure auditability. Bitcoin-like addresses are used to uniquely identify interacting nodes, and authorization tokens are implemented by means of digital signatures to assign access rights. Access control policies are enabled via smart contracts; therefore, each access to resources constitutes a transaction that is verified and validated by miners in the blockchain network.

6. Healthcare

Information and communication technology (ICT) is enabling an emerging generation of intelligent healthcare delivery models that are integrated, holistic, personalized, and even mobile [22]. However, patient-contentedness requires informed decision-making processes that are shared among care providers. This can only be achieved throught seamless access to relevant siloed information held in discrete Electronic Medical Record (EMR) systems [22]. Nevertheless, current systems fall short because of their heterogeneity and the inconsistencies across EMR systems in terms of security policies and access control models [22]. Blockchain technology is seen as offering promising possibilities for a technological revolution, and thus, is seeing an increasing wave of interest in its application in healthcare. Although the limited work reported is still premature, there are a number of promising proposals that may contribute to enabling personalized care through blockchain-based EMR solutions.

Azaria et al. [23] proposed MedRec to overcome the existing barriers and threats to effective cross-organizational information-sharing caused by legacy healthcare information systems or traditional EMR systems. This should eventually address miscommunication issues between patients and healthcare providers; this is to prioritize patient's involvement in their care and reduce third-party direct involvement. It handles a unified patient-centered EMR using a decentralized blockchain-based record management system that is integrated with the patient's healthcare providers. Using permission management, it sustains and secures the network via proof-of-work by various medical stakeholders with the incentives to becoming the blockchain miners. As a reward, MedRec provides access to aggregate and anonymized data. The proof-of-work algorithm is based on a trustless model that is used to secure the content from tampering, where individual nodes must compete to solve computations before the next block unit is added. This creates a comprehensive, immutable accessible log to the patient's medical information across providers and treatment sites.

By contrast, Yue et al. [24], AlOmar et al. [25], and Xia et al. [26] revolutionized EMR systems by enforcing tighter security countermeasures for access control. Yue et al. [24] proposed Healthcare Data Gateway (HGD) as a blockchain solution that gives patients control and access rights to their medical data. Access in HGD is more controlled than in

MedRec as it is based on more strict purpose-based information access scheme. The EMRs in HGD are managed using a blockchain-based storage system that authenticates all data access requests based on a purpose-centered information security principle. In addition, it utilizes a secure Multi-Party Computation (MPC) mechanism to allow third parties to process patient data without risking patient privacy. Meanwhile AlOmar et al. [25] proposed MediBchain, which is similar to HGD in that it revolutionizes EMR systems by using secure countermeasures for authentication but with extra focus on the identification of participants. In addition, Xia et al. [26] proposed MeDShare which adds an extra layer of protection by monitoring entities that access data for malicious use from a data custodian system. This is achieved by employing smart contracts and an access control mechanism to effectively track the behaviour of data.

Although the solutions may vary in their approach or security aspect, they share commonalities in the content and type of blockchain. All of the frameworks care to store transactions in relation to a patient's medical information that needs to be accessed to make an informed decision about the best treatment options. This blockchain is distributed among EMR systems at various healthcare settings based on permissioned blockchain solutions which allow access to only invited, and hence verified users, which complies with information security and data protection laws and regulations for medical record [27].

7. Supply Chain Management

Every day, billions of products are manufactured and shipped to end customers all over the world. Prior to delivery, products travel through a network of retailers, distributors, transporters, storage facilities, and suppliers, which constitute a supply chain. A failure in the supply chain can disrupt operations, potentially leading to financial and reputation losses as well as environmental damage. The complexity of supply chain management demand transparency and traceability to enable risk reduction by increasing awareness of cause-effect relations [28]. In current practice, the storage of trusted information is maintained centrally by a third-party organization, which increases the risks related to technical reliability in data storage and interoperability, security and privacy of the data. The integration of a blockchain solution has the potential to improve process flows and accountability between buyers and suppliers [29].

A blockchain solution for a manufacturing supply chain has been considered [30]. A private blockchain framework was proposed that is designed to provide a shared transparent system that is accessible by supply parties via smart contracts. Each party can join the network through a registration service that verifies identity and qualifications. After this, registered parties have permission to access, write to, and read the blockchain using their private keys. During the supply process, five categories of data are recorded: timestamp, product information, chronological location, chronological ownership, and environmental impact on products. Unlike in the original validation process, any new supply record will be validated when a product is shipped to a new party and both parties sign the smart contract to verify the exchange.

Perishable products are typically sensitive to temperature and storage conditions. A blockchain solution was proposed to ensure the transparency of life-cycle information via shared records, smart contracts, and sensors [31]. Via a registration service, users can obtain public and private keys with which to access the network and maintain their privacy. The stored data are of two categories: user profiles, which stores information about a user, location, certification and association with products, and product profiles, which store product specifications and processing updates. An application scenario with six nodes, namely, production, processing, warehousing, cold chain distribution, retail, and authority organization, was examined. The advantage of using a decentralized system for a food supply chain is to prevent information fraud and extortion by providing transparency, reliability, and security.

In addition to the traceability and tamper-proof nature of records provided by blockchain-based supply systems, adaptability to environmental impacts is an important issue. OriginChain is a private blockchain system that is designed to be adaptable to changing environments and regulations [32]. Data in OriginChain originate from four types of nodes: supplier or retailers; test laboratories; traceability service providers; and factory or freight-yard examiners. To permit various parties to use the blockchain, administration personnel verify parties' requests and issue certificates for access, factory examiners check factories' qualifications, and freight-yard examiners check products and supervise the loading and sealing of products. All information is registered and validated via smart contracts and legal agreements between parties in the supply chain.

8. Government

Electronic government (i.e., e-government) refers to the use of ICT to provide citizens with access to public services [33]. Their aim is to build services around citizens and residents, make government services more accessible, incorporate social aspects, share information responsibly, and utilize resources effectively [34]. This is accomplished by creating a virtual e-government to accelerate the process. Governments have also shown great interest in implementing and improving their e-government services in general, and recently, considerable attention has been directed toward the adoption of blockchain technology to overcome various limitations and improve the running of services.

The government of the United Arab Emirates (UAE) has also taken steps of establishing a Global Blockchain Council to promote the use of blockchain among its services [35]. Some of the reported blockchain projects are focused on particular governmental services, such as e-democracy [34], e-residency [36] or land registration [37], while other projects are focused on the broader use of this technology in solutions for national and international identity management [38] and national data centers [39]. Dubai Blockchain Strategy project is a new technology project which aims to position the UAE as a global distribution that includes all aspects from e-democracy to smart tourism [40] .

The European network TrustedChain is the first and largest authorized blockchain network currently in operation. It supports e-government in addition to other applications [41]. However, its adoption at an international level will require significant efforts, involving additional legislation and standardization [41]. The Republic of Estonia is currently running several e-government programs using blockchain technology. Examples include the Estonian e-residency [36], data sharing [42] [43], and land registry [37] projects. They are intended to provide data owners with personal control over their data to build citizens' trust through an open and transparent secure infrastructure [43]. The project launched by Chancheng in 2014 is the first blockchain government project in China; it is a general application platform for maintaining citizen's digital identities for use by various government institutions [38].

9. Discussion

Initially, cryptocurrencies and financial services were the primary drivers behind blockchain technology. Since then, the technology has expanded to new territories and digital sectors (RQ1). A network analysis of the literature highlighted four of these new environments: in order of keyword frequency, IoT, healthcare, supply chain management, and government. The rest of this section discusses the implications of adopting blockchain technology for each of the four sectors/enviornments.

Internet of Things. Security and privacy are two of the main challenges that IoT systems face due to their inherent characteristics. The three main security requirements of confidentiality, integrity, and availability have been analyzed for the use case of a lightweight smart home [20]. Confidentiality and integrity were found to be achievable via symmetric encryption and hashing, respectively. The use of blockchain also limits the characteristics of acceptable transactions and thus offers protection from malicious requests and ensures availability. These advantages are further exemplified by two additional use cases [19], [21]. The decentralized nature of blockchain supports IoT privacy while also ensuring anonymity and transparency [21].

The integration of blockchains with IoT is still in its infancy and issues still remain to be overcome. Computational overhead is one of these challenges due to the low capabilities of IoT devices. In one case, this issue has been addressed by eliminating the proof-of-work strategy and the concept of coins [20]. Similarly, the lightweight nature of IoT devices translates to limited storage capacities, and thus, data cannot be stored for long periods of time [21]. This issue is closely related to the scalability concerns, as it rapidly becomes expensive for IoT devices to store a growing number of transactions. This also raises concerns regarding the latency of transactions [19], [20], [21]. A layered architecture has been proposed as a future solution to reduce latency, computational overhead, and storage overhead by allowing the partial maintenance of a blockchain [21]. Ultimately, the contradictory nature of these two technologies, although beneficial at times as briefly discussed, is still likely to delay their integration, as evidenced by the low number of use cases despite the relative frequency of the related keywords.

Healthcare. Although most of the work done on the use of blockchain in healthcare started only in 2016, it shows promise for fully supporting a patient-centered care delivery model. However, there are two sides to every coin. The majority of digital immigrants are technologically illiterate, and this new blockchain-based model of care will not be as effective if patients are not competent. On the other hand, there is an increasing demand for user-centered engagement, mainly from digital natives, and thus, it will happen sooner or later. This is clearly evidenced by the European General Data Protection Regulation (GDPR), which empowers users by giving them the right to consent and requires compliance from all organizations serving them in all sectors. This renders blockchain-based permission-controlled access to EMR systems by patients a powerful tool.

Very limited solutions try to work with the challenges of traditional EMR systems by taking an evolutionary approach towards patient-centredness. While remaining frameworks, which seems to be favored, follow a revolutionary approach that discards traditional systems and replace them with new unified blockchain-based EMR framework that is flexible and scalable. Consequently, solutions following the former approach are more relaxed in terms of their security to incorporate brittle inflexible EMR systems, while latter proposals have more flexibility to tighten their security countermeasures. This can be justified due to the fact that traditionally EMR systems are well secured in their local physical perimeters using local organization-oriented policies and access control [22]. However, according to a study in [22], patient-centric movement has caused those systems to compromise on the availability of patient information. Leaving no option to solutions other than relaxing information security countermeasures.

Supply Chain Management. The need for transparency and traceability of products within a supply chain is a primary driver of blockchain utilization, as the auditable nature of this technology facilitates the visibility of transactions to authorized parties [30], [32]. A decentralized solution is especially valuable for perishable goods supply chains as it prevents fraud and extortion by providing data transparency, reliability, and security [31]. One of the main causes of risk to a supply chain is the rapidly changing nature of the relevant environments and businesses, which necessitates proficient adaptability, a challenge that is addressed and mitigated by one of the use cases [32]. The immutability and irrevocability of the data serve as a distributed source of truth when data are exchanged independently by various parties in the supply chain. This overcomes the lack of end-to-end visibility that would otherwise increase fraud risk [31]. Consequently, customers can make better buying decisions, and manufacturers can more closely focus on the quality of their products and on developing better marketing policies [30].

Despite these benefits, the application of blockchain technology in supply chain systems requires a certain technological infrastructure at each party's site in order to keep the system updated [30]. One solution for overcoming the challenges of maintaining up-to-date records and interoperability is to utilize technologies such as sensors, thereby effectively enhancing the continuity of information. The most challenging problem arising with blockchain solutions is the increasing amounts of computation power and storage capacity required as the network expands to achieve the global connectivity necessitated by the trend of globalization. To overcome this challenge, one of the use cases [32] uses on-chain records (hashes of traceability certificates and traceability regulation information) and off-chain records (traceability certificates and the addresses of smart contracts) to manage the balance between performance and privacy. Other challenges also stem from the nature of legacy supply chain systems, including the immaturity of the technology, the need to update current supply technologies, and the training practices in current systems.

Government. The primary driver behind adopting blockchain technology for the government sector is its aim to support an open, transparent, and collaborative government that can streamline access to public services and contract management. In government sectors, information about individuals and organizations can be at risk of isolation within organizational silos. The immutability, transparency, and decentralization of these records promote reliable and efficient data sharing where access to data is controlled. Blockchain technology supports audibility and enforces accountability; in the government sectors, this serves to overcome administrative shortcomings. All of these benefits of blockchain adoption can greatly profit truly networked governments, thus eliminating bureaucracy, fraud and corruption in public services [41], [44], [45]. As evidenced in the cases previously mentioned, the adoption of blockchain has been led by the Eastern European government, principally Estonia [34], [43] and UAE follows with various efforts (e.g. [35]). Other countries such as China, Sweden, Netherlands, Belgium, and Norway have either developed or planned e-government projects utilizing blockchains. It has also been argued that the utilization of blockchain in e-government helps promote the country itself [44], [45].

Nevertheless, the widespread adoption of blockchain technology by government sectors is still limited by numerous technical and legal constraints, as its applications are still immature. Security and privacy concerns are two often cited challenges for the adoption of the blockchain, which have risen due to the recent security Bitcoin breach. It has been argued that the security concern could be overcome by having citizens control their ledger [43]. The lack of regulations is also a setback to blockchain use, particularly to those concerned about information sharing and reporting. Laws will also need to be put forth to govern smart contracts. Technical barriers remain a concern when it comes to the adoption of blockchain technology in the government sector, particularly concerning the set-up cost and the complexity of governance at a national or international level [45]. Once this is overcome, computational overhead and storage concerns issues arise when it comes to maintaining functional systems. These can potentially be combatted with a lightweight scheme that can pilot its success.

10. Conclusion

This paper reports the results of a literature review conducted to investigate the progression of blockchain utility beyond theory in frequently addressed corporate, governmental, and cross-industry environments. Blockchain technology has shown the potential to transform the IoT, healthcare, supply chain management, and government sectors by virtue of its unique characteristics. A review of the literature was conducted for each of these digital sectors to identify use cases of blockchain technology and to assesses its practicality. Furthermore, the benefits and challenges arising for each of these digital sectors were identified from the literature. This paper contributes to the body of research on blockchain technology by highlighting current investigations and thus identifying potential research gaps that could benefit industry if properly addressed. However, questions remain regarding the value of blockchain technology in terms of the experiences of users, namely, the end users at the other end of the continuum.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf [Accessed: 29-03-2018]

[2] Financial Times, "Technology: Banks seek the key to blockchain," 2015. [Online]. Available: https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64 [Accessed: 18-04-2018]

[3] G. Pîrlea, "A review of the blockchain literature," 2016. [Online]. Available: http://students.cs.ucl.ac.uk/2016/group15/reports/research.pdf [Accessed: 19-03-2018]

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in IEEE International Congress on Big Data (BigData Congress). IEEE, 2017, pp. 557–564.

[5] A. Ojo and S. Adebayo, "Blockchain as a next generation government information infrastructure: A review of initiatives in D5 countries," in Government 3.0–Next Generation Government Technology Infrastructure and Services. Springer, 2017, pp. 283–298.

[6] 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, 2016, p. e0163477.

[7] B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, "A critical review of blockchain and its current applications," in International Conference on Electrical Engineering and Computer Science (ICECOS). IEEE, 2017, pp. 109–113.

[8] S. Cao, Y. Cao, X. Wang, and Y. Lu, "A review of researches on blockchain," in the 6th Wuhan International Conference on E-Business Digital Innovation, 2017, pp. 108–117.

[9] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," in International Conference on Exploring Services Science. Springer, 2017, pp. 12–23.

[10] S. Kushch and F. P. Castrillo, "A review of the applications of the block-chain technology in smart devices and distributed renewable energy grids," Advances in Distributed Computing and Artificial Intelligence Journal, vol. 6, no. 3, pp. 75–84.

[11] P. Ghuli, U. P. Kumar, and R. Shettar, "A review on blockchain application for decentralized decision of ownership of iot devices," Advances in Computational Sciences and Technology, vol. 10, no. 8, 2017, pp. 2449–2456.

[12] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2016, pp. 1–6.

[13] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in IEEE EUROCON 17th International Conference on Smart Technologies. IEEE, 2017, pp. 763–768.

[14] Y. Li, T. Marier-Bienvenue, A. Perron-Brault, X. Wang, and G. Paré, "Blockchain technology in business organizations: A scoping review," in the 51st Hawaii International Conference on System Sciences, 2018, pp. 4474–4483.

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

[16] L. Linn and M. Koo, "Blockchain for health data and its potential use in health it and health care related research," in ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, 2016.

[17] T. Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," 2015. [Online]. Available: https://www.weusecoins.com/assets/pdf/library/Consensus-as-a-service [Accessed: 10-12-2017]

[18] A. Knutas, A. Hajikhani, J. Salminen, J. Ikonen, and J. Porras, "Cloud-based bibliometric analysis service for systematic mapping studies," in the 16th International Conference on Computer Systems and Technologies. ACM, 2015, pp. 184–191.

[19] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for IoT updates by means of a blockchain," in IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2017, pp. 50–58.

[20] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2017, pp. 618–623.

[21] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," Security and Communication Networks, vol. 9, no. 18, 2016, pp. 5943–5964.

[22] S. Alsalamah, H. Alsalamah, A. W. Gray, and J. Hilton, "Information security threats in patient-centred healthcare," in M-Health Innovations for Patient-Centered Care. IGI Global, 2016, pp. 298–318.

[23] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in International Conference on Open and Big Data (OBD). IEEE, 2016, pp. 25–30.

[24] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, 2016, p. 218.

[25] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, 2017, pp. 534–543.

[26] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, 2017, pp. 14 757–14 767.

[27] S. Alsalamah, "Information classification scheme for next generation access control models in mobile patient-centered care systems," in the 12th International Conference on Cyber Warfare and Security (ICCWS'17), 2-3 March, Dayton, USA, 2017, pp. 1–9.

[28] M. Frentrup, L. Theuvsen et al., "Transparency in supply chains: Is trust a limiting factor," Trust and Risk in Business Networks, ILB-Press, Bonn, 2006, pp. 65–74.

[29] S. Asharaf and S. Adarsh, Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities: Emerging Research and Opportunities. IGI Global, 2017.

[30] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," International Journal of Research in Engineering and Technology, vol. 5, no. 9, 2016, pp. 1–10.

[31] F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology," in the 13th International Conference on Service Systems and Service Management (ICSSSM). IEEE, 2016, pp. 1–6.

[32] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," IEEE Software, vol. 34, no. 6, 2017, pp. 21–27.

[33] S. Stier, "Political determinants of e-government performance revisited: Comparing democracies and autocracies," Government Information Quarterly, vol. 32, no. 3, 2015, pp. 270–278.

[34] T. V. Kumar, E-Democracy for Smart Cities. Springer, 2017.

[35] Government of Dubai, "Dubai Museum of the Future Foundation announces launch of Global Blockchain Council," 2016. [Online]. Available: http://mediaoffice.ae/en/media-center/news/17/2/2016/dubai-museum-of-the-future-foundation-announces-launch-of-global-blockchain-council.aspx [Accessed: 12-04-2017]

[36] C. Sullivan and E. Burger, "E-residency and blockchain," Computer Law & Security Review, vol. 33, no. 4, 2017, pp. 470–481.

[37] C. Lemmen, J. Vos, and B. Beentjes, "Ongoing development of land administration standards," European property law journal, vol. 6, no. 3, 2017, pp. 478–502.

[38] H. Hou, "The application of blockchain technology in e-government in china," in the 26th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2017, pp. 1–4.

[39] M. Chibuye and J. Phiri, "Blockchain–its practical use for national data centres," Zambia ICT Journal, vol. 1, no. 1, 2017, pp. 57–62.

[40] M. S. Khan, M. Woo, K. Nam, and P. K. Chathoth, "Smart city and smart tourism: A case of dubai," Sustainability, vol. 9, no. 12, 2017, p. 2279.

[41] M. Atzori, "Blockchain governance and the role of trust service providers: The Trustedchain ® network," 2017. [Online]. Available: https://ssrn.com/abstract=2972837 [Accessed: 12-04-2017]

[42] S. Witherden, "Exploring different approaches to data sharing."

[43] J. Priisalu and R. Ottis, "Personal control of privacy and data: Estonian experience," Health and technology, vol. 7, no. 4, 2017, pp. 441–451.

[44] N. Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the global south?" Third World Quarterly, vol. 38, no. 8, 2017, pp. 1710–1732.

[45] H. Zhu and Z. Z. Zhou, "Analysis and outlook of applications of blockchain technology to equity crowdfunding in china," Financial Innovation, vol. 2, no. 1, 2016, p. 29.