Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

Scientometric Study on Distributed Ledger Technology (Blockchain)

Mike Culhane
National Research Council (NRC)

Prepared by:
National Research Council (NRC)
1200 Montreal Road, Building M-58
Ottawa, Ontario
K1A 0R6 Canada

MOU: National Research Council of Canada (NRC) concerning Research, Development, Test and Evaluation, Technical Services and CoOp RD

Other Contract Number: FE22071907
Technical Authority: Alain Auger, Defence Scientist
Contractor's date of publication: November 2018

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2019-C059
March 2019

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

NRC·CNRC

Scientometric Study on Distributed Ledger Technology (Blockchain)

Prepared for:
Alain Auger, Lead, S&T Outlook, Office of the Chief Scientist
Francine Desharnais, Chief Scientist, Information Sciences
Joelle Thorpe, Policy Analyst, Office of the Chief Scientist

Prepared by:
Mike Culhane, Intelligence Analyst
Intelligence and Analytics, National Science Library
National Research Council (NRC)

Date: November 30, 2018

NRC-NSL Project Number: MC19-005

DRDC Project Number: FE22071907

National Research Council Canada | Conseil national de recherches Canada

Canada

[This page intentionally left blank]

Table of Contents

1 EXECUTIVE SUMMARY 5

2 BACKGROUND 6

2.1 CONTEXT 6
2.2 KEY QUESTIONS 6

3 INTRODUCTION 7

3.1 DEFINITION 9

4 LITERATURE ANALYSIS 10

4.1 TEMPORAL DISTRIBUTION 10
4.2 TOP COUNTRIES 11
4.3 TOP AUTHOR AFFILIATIONS 12
4.4 COLLABORATION NETWORKS 14
4.5 KEYWORD CLUSTER MAP 16
4.6 MAJOR TOPICS 18
4.7 AREAS OF RESEARCH INTEREST—CANADIAN AUTHOR AFFILIATIONS 19
4.8 AREAS OF RESEARCH INTEREST—MILITARY AUTHOR AFFILIATIONS 20
4.9 RESEARCH MOMENTUM 22
4.9.1 Military Applications 27
4.9.2 Government Applications 33

5 BARRIERS AND CHALLENGES 37

6 CONCLUSION 40

7 REFERENCES 42

8 APPENDICES 51

8.1 ATTACHMENTS 51
8.2 METHODOLOGY 51
8.2.1 Search Strategy 51
8.2.2 Analysis 51
8.2.3 R&D Momentum 51

List of Figures

Figure 1. Temporal Distribution, Literature 10
Figure 2. Top Countries 11
Figure 3. Top Author Affiliations 12
Figure 4. Top Canadian Affiliations, No. of Publications 14
Figure 5. Co-Publication Network 15
Figure 6. Keyword Cluster Map 17
Figure 7. Top Subject Groups, Literature 18
Figure 8. Canadian Organizations, Areas of Research Interest 19
Figure 9. Military Affiliations, Areas of Research Interest 20
Figure 10. Research Momentum, Literature Subject Groups 23
Figure 11. Research Momentum, Hot Topics Quadrant 24
Figure 12. Research Momentum, Emerging Topics Quadrant 25
Figure 13. Research Momentum, Brand New Topics Quadrant 26
Figure 14. Temporal Distribution, Government Publications 33

List of Tables

Table 1. Top Author Affiliations By Type (No. of Publications) 13

1 EXECUTIVE SUMMARY

DRDC commissioned this scientometric study on distributed ledger technology (DLT) with a view to understanding the potential impact of new research on future security and defence capabilities and operations. To answer the questions posed in the mandate, publication references from the past 10 years were retrieved and analyzed using text mining software and a variety of information visualization tools.

In total, 2,520 journal articles, conference papers, theses, books and government reports were published on DLT in the scientific literature between January 1, 2008 and October 1, 2018, and the number is growing rapidly. Just over 51% have been published so far in 2018 alone, a testament to the velocity of research interest recently. An analysis of an aggregated field of keyword subject groups created from the set of 2520 documents shows that some of the primary topics of R&D interest are cryptocurrencies, data security, applications and the Internet of Things. The top publishing author-affiliations are the Chinese Academy of Sciences (49 publications), IBM (48) and Australia's CSIRO (36). In Canada, the University of British Columbia is the most prolific entity, with 11 publications. The top military-related organizations in the dataset are China's National University of Defense Technology (19 publications), the US Air Force Research Laboratory (11) and the US Army Research Laboratory (5).

According to the literature, potential applications of distributed ledger technology, in particular blockchain, appear to be almost limitless and are projected to radically impact many industries in the coming years. For governments, DLT could help to streamline healthcare delivery, improve the collection of taxes, issue more secure passports and generally ensure the integrity of government records and services. For defense and security organizations, the technology promises to make supply chains more secure and efficient, protect sensitive data and communications, and enable more effective identity management.

However, despite the recent enthusiasm and surge of DLT initiatives around the world, whether the technology will live up to the lofty expectations is still up for debate. Several barriers and challenges remain, such as regulatory concerns, energy requirements and whether a blockchain without a native currency is even viable, or can provide a better solution than existing technology.

2 BACKGROUND

2.1 Context

In order to assist with long-term R&D planning and the prioritization of research topics, scientometric studies are being commissioned by DRDC to provide a high-level overview of global research and development activity in certain scientific domains. These studies will assist DRDC and its partners in uncovering and understanding the potential impact of new research on future defense and security capabilities and activities.

To that end, this scientometric study focuses on the topic of distributed ledger technology (often used synonymously with blockchain) and its impact on national defence and security. It is designed to provide a comprehensive overview of the domain through an analysis of the literature, in order to frame and inform future DRDC goals and projects related to the topic.

2.2 Key Questions

1. Over the past ten years, what are the major research topics described in the scientific and technical literature in the area of distributed ledger technology (DLT)*?*
2. What are the existing and potential future defence and national security applications of DLT?
3. Have any other government departments (inside or outside of Canada) adopted DLT beyond the pilot phase, and have any cost/benefit studies been conducted with respect to implementing DLT in government?
4. What are the barriers, challenges and risks to implementation of DLT?
5. Based on publication volume and rate of increase for research subjects, which topics are emerging?
6. Who are the major players publishing in the area? What is the nature of their expertise?
7. What are the major international collaboration clusters?
8. What are the SPEED (Social, Political, Economic, Environmental and Defense) impacts of distributed ledger technology?

3 INTRODUCTION

> *Blockchain technology can be viewed as the fifth paradigm of computing technology following the mainframe, the personal computer, the Internet and finally the mobile and social network revolution*.[1]
>
> *The Internet is entering a Second Era. The first era was based on information and content being available anywhere and anytime. Now, the second era – powered by blockchain technology – is bringing us the Internet of value: a new, distributed platform that will help us reshape the world of business and transform the old order of human affairs for the better.*[2]
>
> *Blockchain falls into the category of "foundational technologies" – and like the internet or mobile devices before it, it could transform not just what we can do but how we do it, in fundamental ways.*[3]

The attention distributed ledger technology (DLT), especially blockchain, has received recently has been enormous, in part propelled by the meteoric rise of the bitcoin cryptocurrency, a related technology which enables a peer-to-peer version of electronic cash. As the above quotations attest, the attention to blockchain has been accompanied by no shortage of hyperbole and inflated expectations.

First conceptualized in a 2008 paper[4] by a person (or group of persons[a]) named Satoshi Nakamoto, blockchain technology has been hailed as the solution to everything from securing data for businesses to making government services more efficient. In a nutshell, a blockchain is a distributed, highly secure ledger or database where virtually anything—currency, intellectual property, art, music, health records and even votes—can be securely stored and exchanged without the need for a centralized intermediary. The database is shared by group of network participants, all of whom can submit new records for inclusion. Sophisticated algorithms built into the system ensure trust and security among participants, and records are only added to the database based on the agreement, or consensus, of a majority of the group. Once the records are entered on a block, it is extremely difficult to change or delete them.

Applications of blockchain and distributed ledger technologies are proclaimed to be almost limitless, and they are projected to radically impact a wide variety of industries in the coming years.

[a] See "Who is Satoshi Nakamoto?", The Economist, Nov. 2015

The number of DLT projects around the globe have been increasing at a phenomenal rate. New initiatives are announced almost daily, and research interest in DLT (and blockchain specifically) has exploded recently. Over the past two years, major technology vendors—including five of the world's biggest cloud companies—have introduced blockchain-as-a-service. The number of active blockchain consortia across industries has rapidly increased from 28 in 2017 to more than 605 as of October, 2018. In the US, state legislatures have taken action on dozens of blockchain-related bills so far this year, and at least eight states have already passed laws.[6]

By providing a decentralised, consensus-based, immutable record of transactions, distributed ledger technology could transform a number of industries (and industrial processes) when combined with other technologies. For example, DLT could have a significant impact on supply chains, enabling the tracking and tracing of goods and reducing counterfeiting. In the automotive industry alone, firms lose tens of billions of dollars a year to counterfeit parts.[7,8] Canada's Hercules transport aircraft were also found to contain counterfeit parts in their cockpits.[9]

A blockchain could also permit end-to-end encryption of the entire process of designing, transmitting and printing 3-D computer-aided design (CAD) files, with each printed part embodying a unique digital identity and memory.[10] With this stored identity, the blockchain could provide proof of compliance with warranties, licences and standards during production, installation, and maintenance. It could authenticate machine-based data exchanges, implement associated micro-payments, and help monetise the Internet of Things (IoT).[11] In addition, recording machine-to-machine exchanges of valuable information could lead to "data collateralisation", giving lenders the security to finance supply chains and helping smaller suppliers overcome working-capital shortages.[10,8] By providing verifiably accurate data across the production and distribution processes, a blockchain could also enhance predictive analytics.[11]

Blockchain could further automate supply chains through the digital execution of "smart contracts", which rely on pre-agreed obligations being verified automatically. Maersk, for example, is working with IBM to test a blockchain-based approach for all documents used in bulk shipping. Called TradeLens, the technology aims to bring the shipping industry into the digital age through a secure interface exclusively dedicated to freight transport. The Port of Montréal and the Canada Border Services Agency have recently signed on to use TradeLens.[12]

Blockchain could also help to accelerate advances in artificial intelligence (AI). AI applications require a massive (and therefore expensive) amount of computing power. A start-up called Tatau has created a decentralized platform that will allow those in need of AI computational power and storage to purchase it, and those that have surplus quantities, to sell it. FaceMe, a provider of AI-powered 'digital humans' for customer service, and Tatau are working together to increase the speed and scope of the GPU-based processing in FaceMe's advanced AI software.[13,14]

Clearly, there is no shortage of enthusiasm for DLT, and in particular blockchain. Military organizations around the world are also investigating the technology. But will reality live up to the hype?

3.1 Definition

In the mainstream media as well as the research literature, multiple terms related to DLT are often conflated and misused, adding to the confusion about what DLT (and a blockchain) actually is and potentially generating incorrect assumptions about what these technologies can and cannot do.

While there is no one standard definition of blockchain, it is most commonly referred to in the literature as a "distributed ledger of transactions". This is why the phrase "blockchain technologies" is often used interchangeably with "distributed ledger technologies" (DLT). At the core, both are simply databases, but there are differences between them. Unlike a typical centralized database run and maintained by a single entity such as a bank or government**,** a distributed ledger is a database that is managed by some or all of the participants. There is no single, central authority that acts as arbitrator or monitor.

Distributed ledgers are a type of distributed database, which have been around for three decades.[16] A distributed ledger can be "permissioned" or "permissionless", depending on whether nodes need permission from any entity to make changes to the ledger. In a permissionless DLT, participation is enabled by relevant software and a server; in permissioned systems, a central administrator controls access and enforces rules. DLTs can also be public or private, depending on whether the ledgers can be accessed by anyone or only by participating nodes in the network. Whatever the design of a DLT, the advantage is that many parties or nodes must confirm a single and up-to-date version of the data, thus ensuring greater accuracy, transparency, and trust.

A blockchain is a *type* of distributed ledger. In other words, every blockchain is a distributed ledger but not every distributed ledger is a blockchain. The uniqueness of a blockchain is that it organizes data into "blocks" and updates the entries using an append-only, immutable structure. It can also set rules about a transaction that are tied to the transaction itself. This contrasts with a conventional database, in which rules are often set at the entire database level, or in the application, but not in the transaction.[17]

Not all distributed ledgers, however, employ (or need to employ) a chain of blocks to provide a secure and valid distributed consensus. For example, in a private distributed ledger system where there are no untrusted members, a blockchain is a poor fit. In fact, some observers attribute the emerging usage of "distributed ledger technology" as an indictment of the fact that blockchain, as it applies in the cryptocurrency world, cannot square with the demands of regulated industries that require privacy, scale, competition, autonomy, legal recourse and compliance. In reality, most "blockchain" ventures today have nothing to do with blockchain as it was originally described or used in bitcoin.[18,b]

A technical review and evaluation of the currently available blockchain systems is outside the scope of this study, but some of the major platforms many organizations are using to build blockchain applications (Ethereum, Hyperledger Fabric, R3 Corda, Ripple, Quaorum, etc.) are mentioned in this report.

[b] For the purposes of this report, unless indicated otherwise, the terms "blockchain" and "distributed ledger technology" will be used interchangeably.

4 LITERATURE ANALYSIS

In order to address the key questions of this study, comprehensive searches in multiple literature databases were conducted in early October, 2018. In all, 2,520 publications (including research papers, conference proceedings, technical reports, books and book chapters) were retrieved, covering the period 2013-2018. The publication metadata (title, author, affiliation, keywords, abstract, etc.) were imported to text-mining software for cleaning, grouping and analysis.

A full description of the databases and methodologies used is provided in the Appendix. In addition, to enable further study, a separate spreadsheet containing the complete publication dataset accompanies this report.

4.1 Temporal Distribution

Figure 1 illustrates the general level of research interest in distributed ledger technology over the time frame analysed. The velocity of publication activity in the past two years is especially pronounced – 2018 alone (despite being incomplete) has more publications than all the previous years combined, and comprises 51% of the dataset.

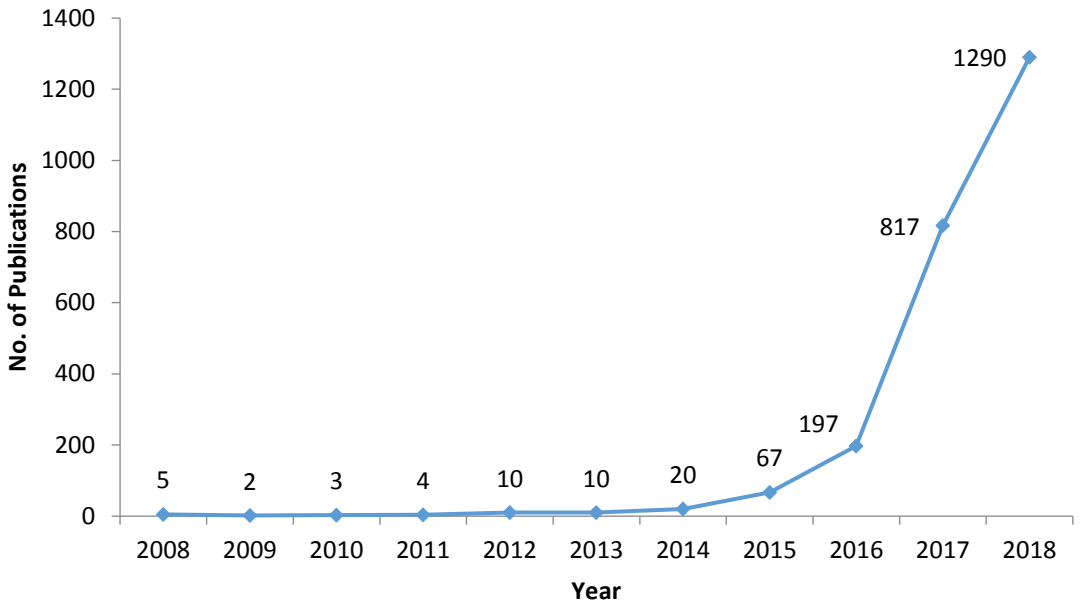

Figure 1. Temporal Distribution, Literature

4.2 Top Countries

There are a total of 5,487 authors in the set, representing organizations from 92 nations. Figure 2 shows the top 20 countries and provides an indication of the global distribution of research and development activity for DLT. The US and China are the dominant players, followed by the UK, Germany and Italy to complete the top five. Canada ranks 12th with 74 publications.

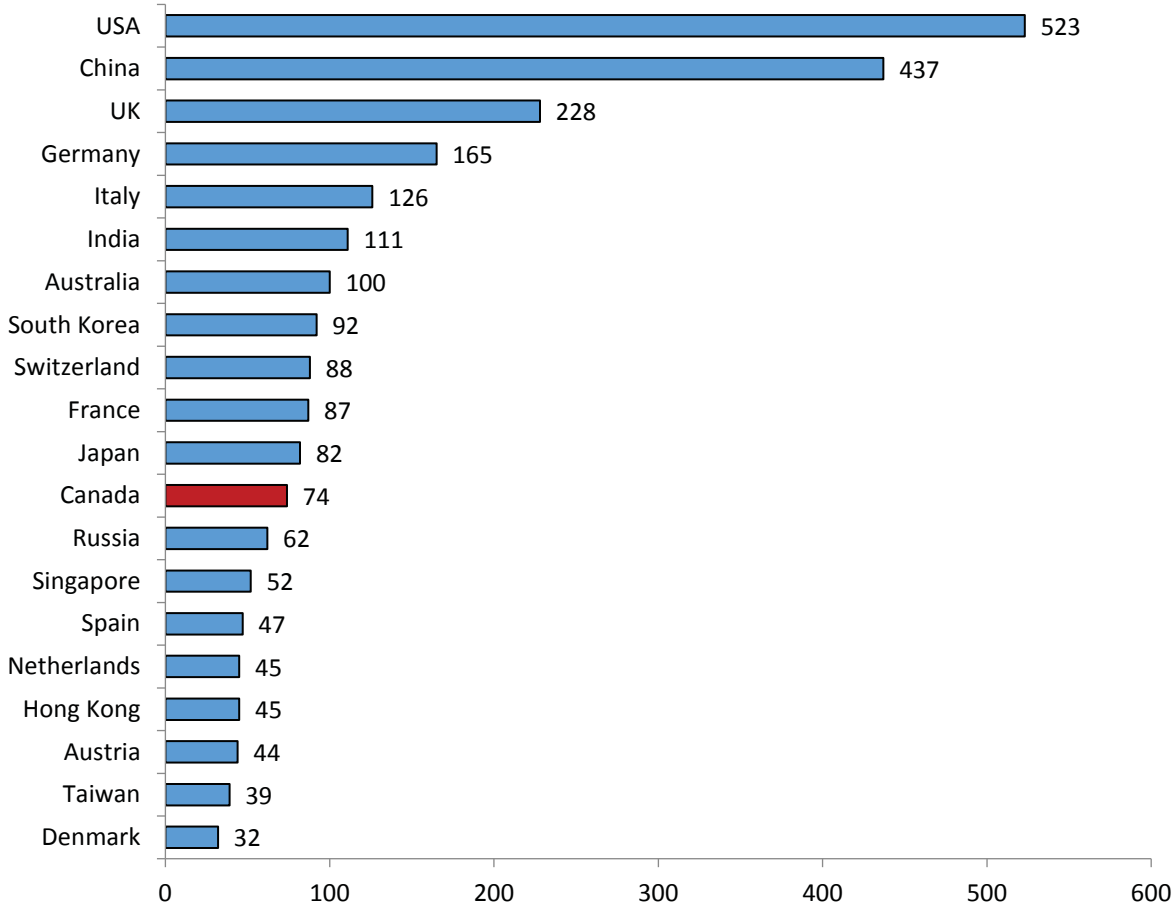

Figure 2. Top Countries

4.3 Top Author Affiliations

Figure 3 shows the top ten author affiliations (from a total of 1,831) for publications in the dataset. The list contains a mixture of academic institutions and national research and technology organizations, with one commercial entity, IBM Corp. (ranked 2nd).

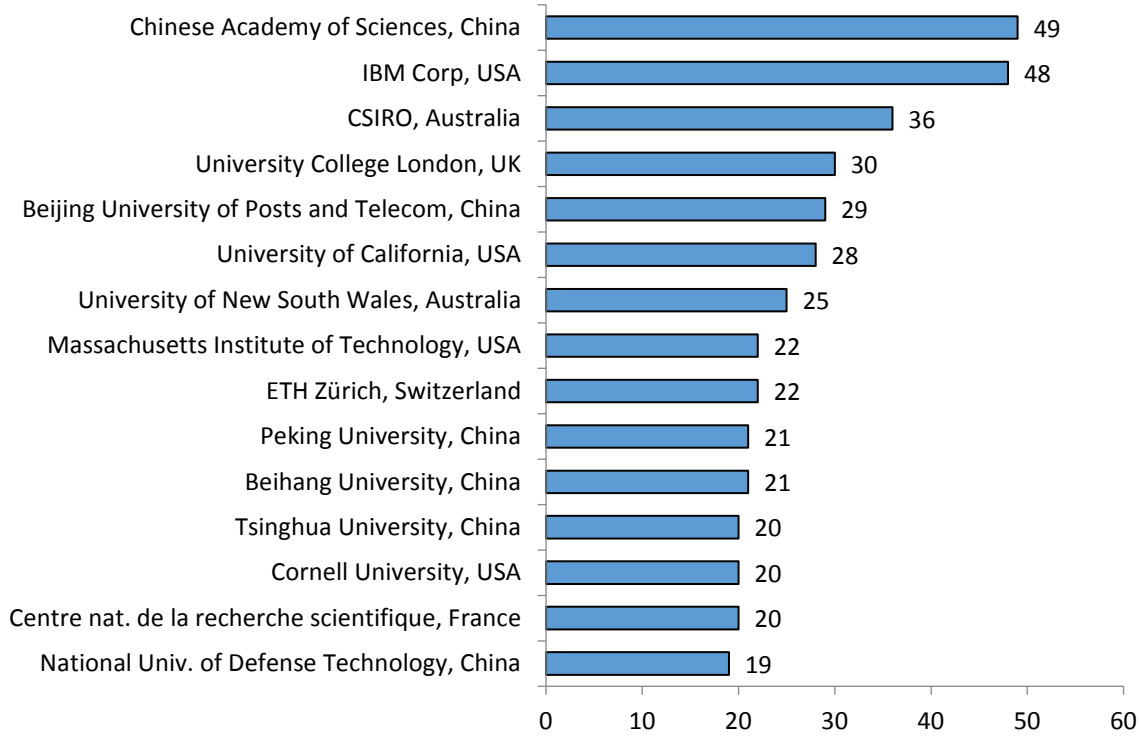

Figure 3. Top Author Affiliations

With 49 records, the Chinese Academy of Sciences (CAS) is the dominant player. Several of the CAS publications are concerned with data security and privacy in IoT applications, such as *Towards data assurance and resilience in IoT using blockchain.* The paper explains that the widespread adoption of UAVs in domains as diverse as warfare, agriculture and package delivery has made the protection and integrity of data and communications between UAVs and the control system increasingly crucial. The researchers propose a distributed solution using blockchain technology along with a traditional cloud server. Instead of registering the drone itself to the blockchain, the data collected from UAVs are anchored to the blockchain network and stored in the cloud. This process is therefore removed from the drone itself, saving battery and processing power while enhancing security of the data.[20]

In another paper from CAS, *Blockchain for large-scale Internet of Things data storage and protection,* the authors present what they describe as the first work designing a secure and accountable IoT data storage system using blockchain. With the dramatically increasing deployment of IoT devices, storing and protecting the large volume of IoT data has become a significant issue. Traditional, cloud-based IoT structures impose extremely high computation and storage demands on cloud servers. Strong dependencies on the centralized servers also bring significant trust issues. To address these problems, the researchers propose a distributed data storage scheme employing blockchain and certificate-less cryptography, thus eliminating the traditional centralized servers by leveraging blockchain miners.[21]

A Blockchain based privacy-preserving incentive mechanism in crowdsensing applications is a 2018 paper co-authored by researchers from CAS and North China University of Technology. Crowdsensing applications are based on data collected from smartphone users, and the quality of the sensing data depends on the participation of a large number of users. To motivate individuals to participate, rewards can be offered to compensate for the use of their device data. The authors of the paper propose a privacy-preserving blockchain incentive mechanism in which a cryptocurrency built on a blockchain is used as a secure motivation mechanism.[22]

Typically, large academic institutions and well-funded national organizations such as CAS tend to publish prolifically, and therefore dominate the top positions in publication output rankings. To get a sense of the activities of some of the smaller, but still important, players in the set, the author affiliations were also classified by type: Military, Commercial, and Government/RTO[c] (Table 1). The publications of some of these organizations will be discussed in more detail in later sections of this report.

Table 1. Top Author Affiliations By Type (No. of Publications)

Military	Commercial	Government/RTO
National University of Defense Technology, China (19)	IBM, USA (48)	CSIRO, Australia (36)
US Air Force Research Laboratory (11)	NEC Corp., Japan (10)	ETH Zürich, Switzerland (22)
US Army Research Laboratory (5)	Nokia, Finland (9)	Centre nat. de la recherche scientifique, France (20)
Defence Research and Development Canada (1)	NTT Corp., Japan (9)	Inst. Nat. de recherche en informatique et en automatique, France (15)
Air Force General Hospital, China (1)	Microsoft, USA (7)	Karlsruhe Institute of Technology, Germany (15)
Defence Institute of Advanced Technology, India (1)	Huawei Technologies Co., China (6)	National University of Singapore (15)
Naval Postgraduate School, USA (1)	KDDI Research Inc., Japan (6)	National Taiwan University (9)
Nikola Vartsarov Naval Academy, Bulgaria (1)	Ergo Platform and IOHK Research, Russian Federation (5)	École Polytechnique Fédérale de Lausanne, Switzerland (9)
US Army Engineer Research and Development Center (1)	nChain, UK (5)	Electronics and Telecom. Research Institute, South Korea (7)

[c] RTO = Research & Technology Organization

The Canadian organizations were also extracted from the dataset (those with three or more records) to illustrate the extent of DLT R&D in Canada (Figure 4). The University of British Columbia is most active with 11 publications, the majority of which emanate from the Blockchain@UBC lab, a collaborative research cluster supported by the Institute for Computing, Information, and Cognitive Systems that focusses on blockchain technology as one component in investigating the broader research question "How can emerging technologies be leveraged to benefit Canadians?"[23]

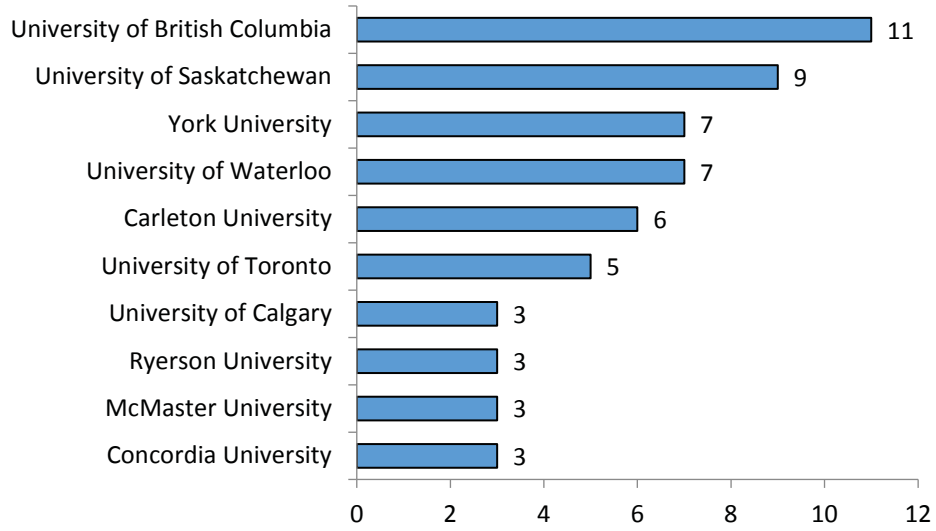

Figure 4. Top Canadian Affiliations, No. of Publications

4.4 Collaboration Networks

With the aim of determining the extent of collaboration among the major organizations in the literature, a network map was created to illustrate the co-publishing relationships of the major players in the set (Figure 5). The nodes (bubbles) are sized according to the quantity of underlying publications, and the number that appears on the connecting line represents the number of co-publications. For clarity, the map has been filtered to only show relationships of the top organizations (overall and by type – Academic, Commercial, Government/RTO, Military and Canadian), with at least two shared publications.

Although co-publication does not necessarily indicate collaboration at an official level, networking patterns can provide insight into working relationships among experts, as well as reveal national or international knowledge networks. The map suggests that a number of these networks appear to be geographically-based, with co-publication occurring among affiliations that are in the same country or region. Most of the Canadian organizations, for example, are co-publishing with other organizations in Canada.

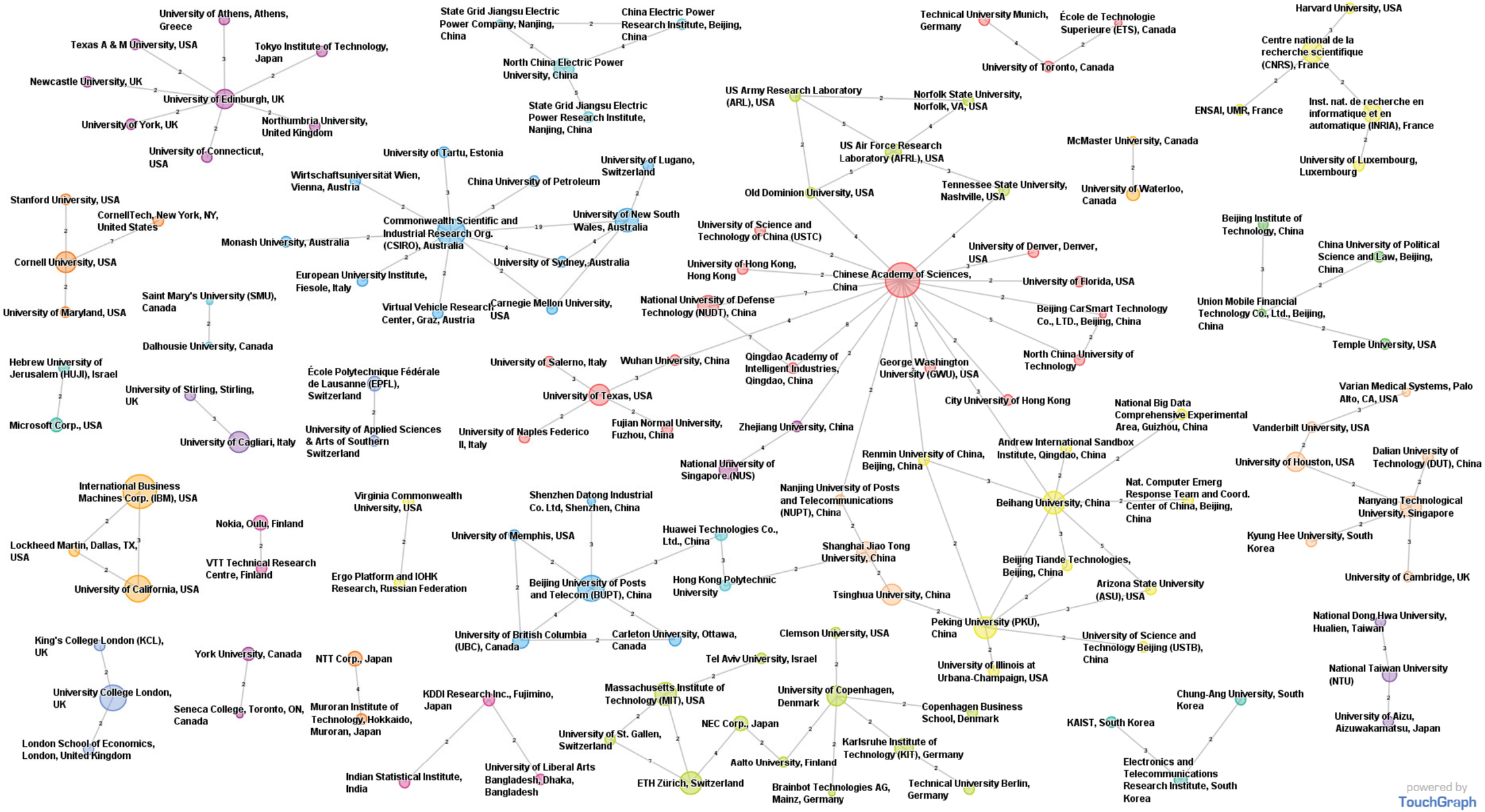

Figure 5. Co-Publication Network

Two of the top three author affiliations in the set, the Chinese Academy of Sciences and Australia's CSIRO, have a large number of collaborations with both national and international partners. Interestingly, IBM, with the second highest number of publications, has collaborations with just Lockheed Martin and the University of California (orange cluster on the far left of the graph). Several of IBM's publications are concerned with Hyperledger Fabric (the platform on which the IBM blockchain product runs) and its application in various industries, such as healthcare[24,25] and insurance.[26,27]

The US Army Research Lab (ARL) and the US Air Force Research Lab (AFRL) share five publications (green cluster of nodes near the top of the image). Others in that cluster are Norfolk State University, Old Dominion University and Tennessee State University. Some of these publications will be explored in more detail in later sections.

4.5 Keyword Cluster Map

As indicated previously, the total number of records retrieved for this study, covering the period 2008-2018, was 2,520. With such a large set of documents it is virtually impossible, via manual methods, to derive meaningful insight into the major concepts and research subjects. Therefore, a series of literature analysis and data mining techniques were employed to delve deeper into the dataset.

First, in order to achieve a "bird's-eye" view of the publications and to detect the major topics and research areas, relationships among the top 300 keywords (originating from the author-supplied and indexed keyword fields in each bibliographic record)[d] were plotted using cluster mapping software (Figure 6). The software's algorithm creates clusters of terms based on statistical similarity to one another (i.e. word co-occurrences). For clarity, the map has been filtered to show autocorrelations of 18% or higher (the correlation percentage is shown on the line between nodes).[e] Like the collaboration map above, the size of each node corresponds to the relative number of underlying publications.

A number of distinct clusters are immediately identifiable in Figure 6. Naturally, the largest cluster in the map is that anchored by *Electronic money* (yellow cluster in the center of the graph) which is connected to other large nodes such as *Bitcoin, Cryptocurrency* and *Cryptography*. *Data privacy* and *Internet of things* are other substantial nodes in the middle of the map, below which is found a blue cluster concerned with health care and electronic medical records. To the left, in green, is a cluster of keywords related to smart grids and energy resources, which is linked to a second cluster concerned with electric vehicles. Above and to the left is a cluster of nodes with publications about supply chains.

As a whole, the map of the top 300 keywords provides a visual representation of the major areas of scientific inquiry in the domain of distributed ledger technology over the past five years, and offers context for the more in-depth analyses of the dataset in the sections that follow.

[d] The total number of keywords from all 2,520 publications is 13,900. The top 300 keywords represents approximately 90% of the dataset.

[e] Correlation values are set at a percentage that enables the graph to be readable while still showing a significant number of clusters. For more information on the clustering algorithm please see https://tinyurl.com/ybgbtjpc.

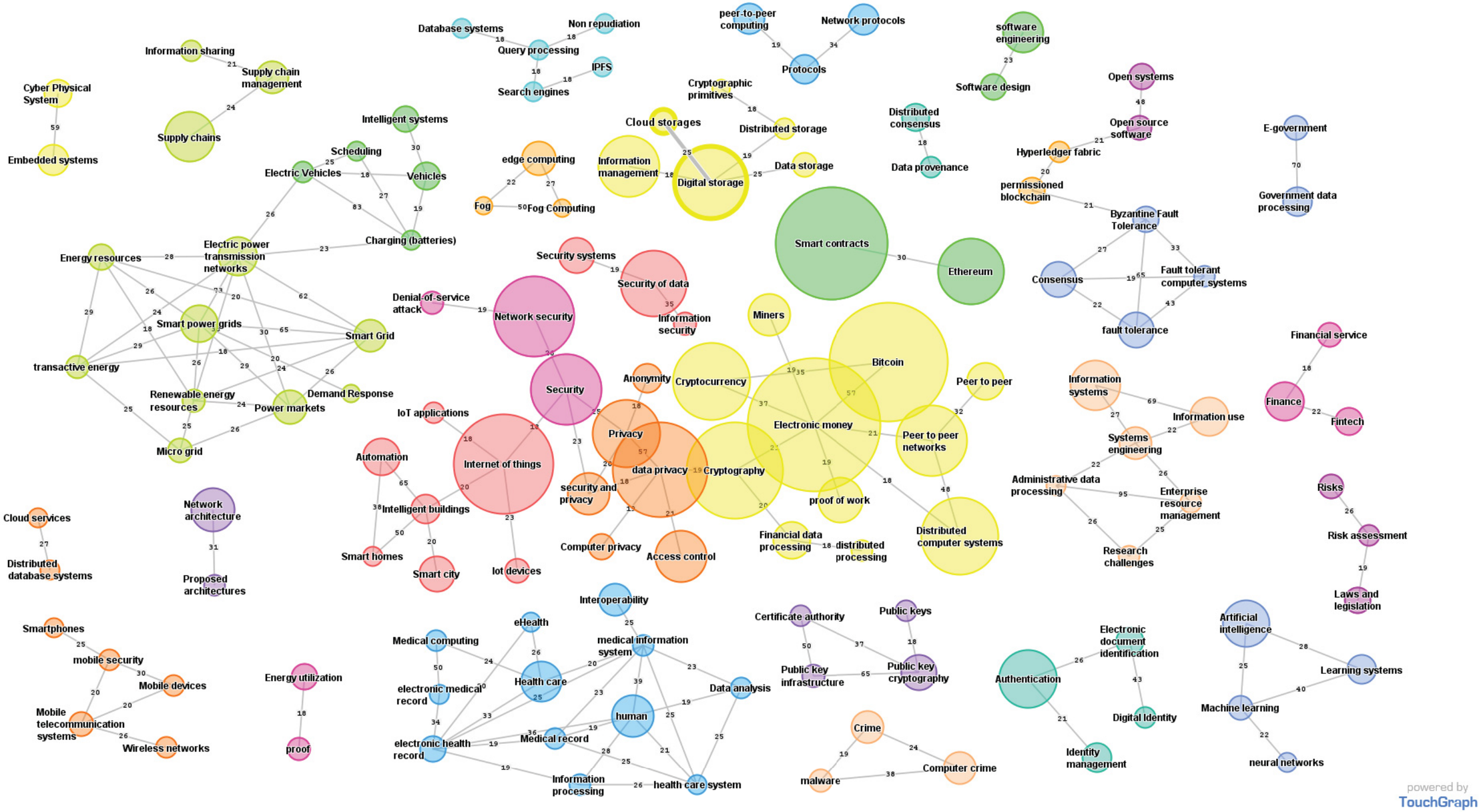

Figure 6. Keyword Cluster Map

4.6 Major Topics

As mentioned, the cluster map shown above provides a visual overview of some of the primary areas of research focus in the scientific literature. In order facilitate a deeper dive into the data, the 13,900 keywords were cleaned, normalized and classified into a total of 60 subject groups, representing 93% of the dataset.[f] These subject groups denote the major research topics of interest in DLT over the past ten years.

Figure 7 displays the top 25 groups and their corresponding number of publications.[g,h]

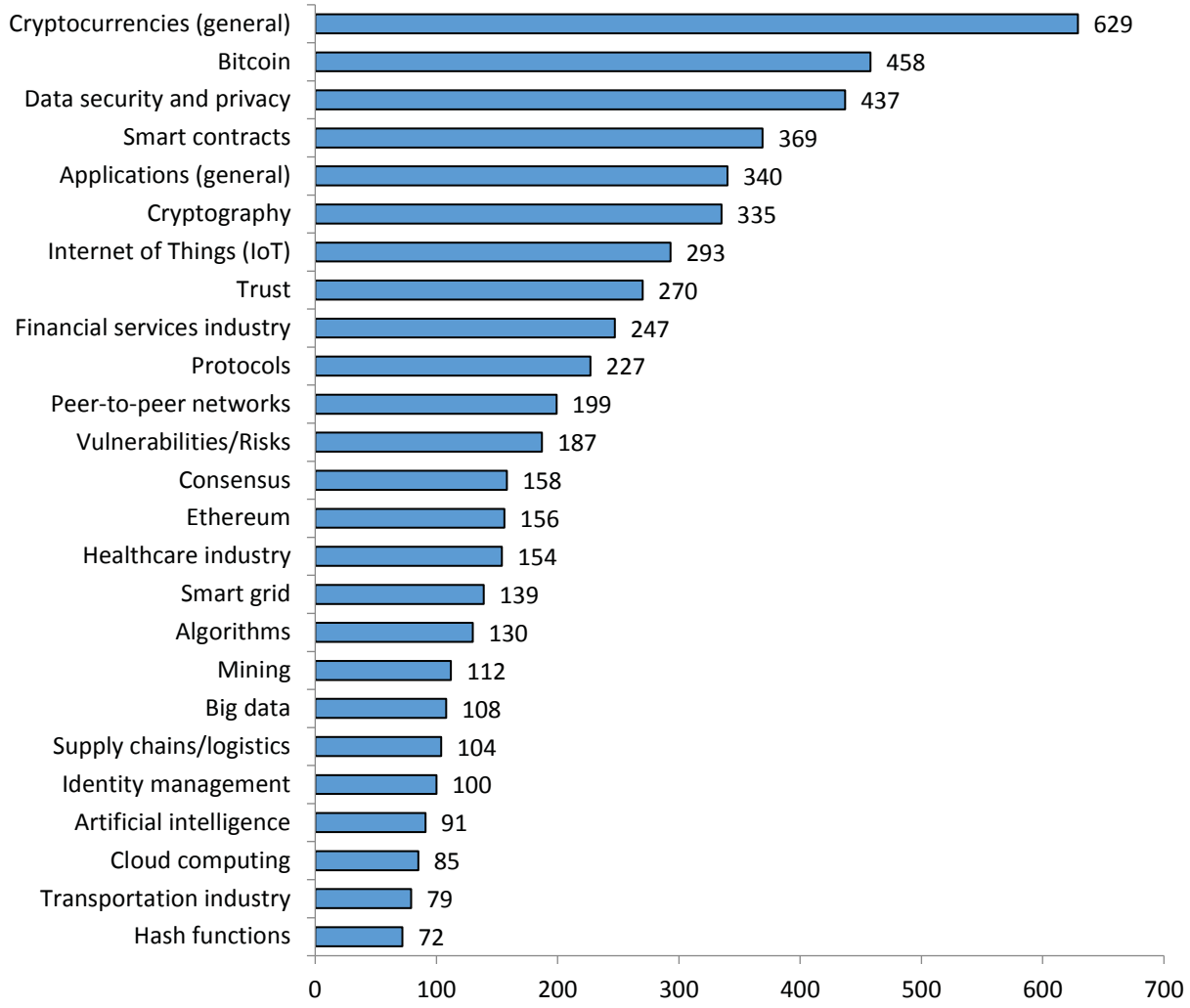

Figure 7. Top Subject Groups, Literature

[f] The subject groups are not mutually exclusive; a publication can belong to one or more groups.
[g] Groups with "(general)" contain non-specific publications about the topic. For example, "Cryptocurrencies (general)" contains publications that discuss cryptocurrencies broadly; i.e. they are not specifically about bitcoin or another cryptocurrency.
[h] All the subject groups and associated publications are available in the Excel file accompanying this report.

4.7 Areas of Research Interest—Canadian Author Affiliations

Using the subject groups, field co-occurrence matrices can be developed to gain insight into the specific areas of research interest of the individual author affiliations. For example, Figure 8 is a co-occurrence map showing the presence of the subject groups in the publications from the Canadian author affiliations.

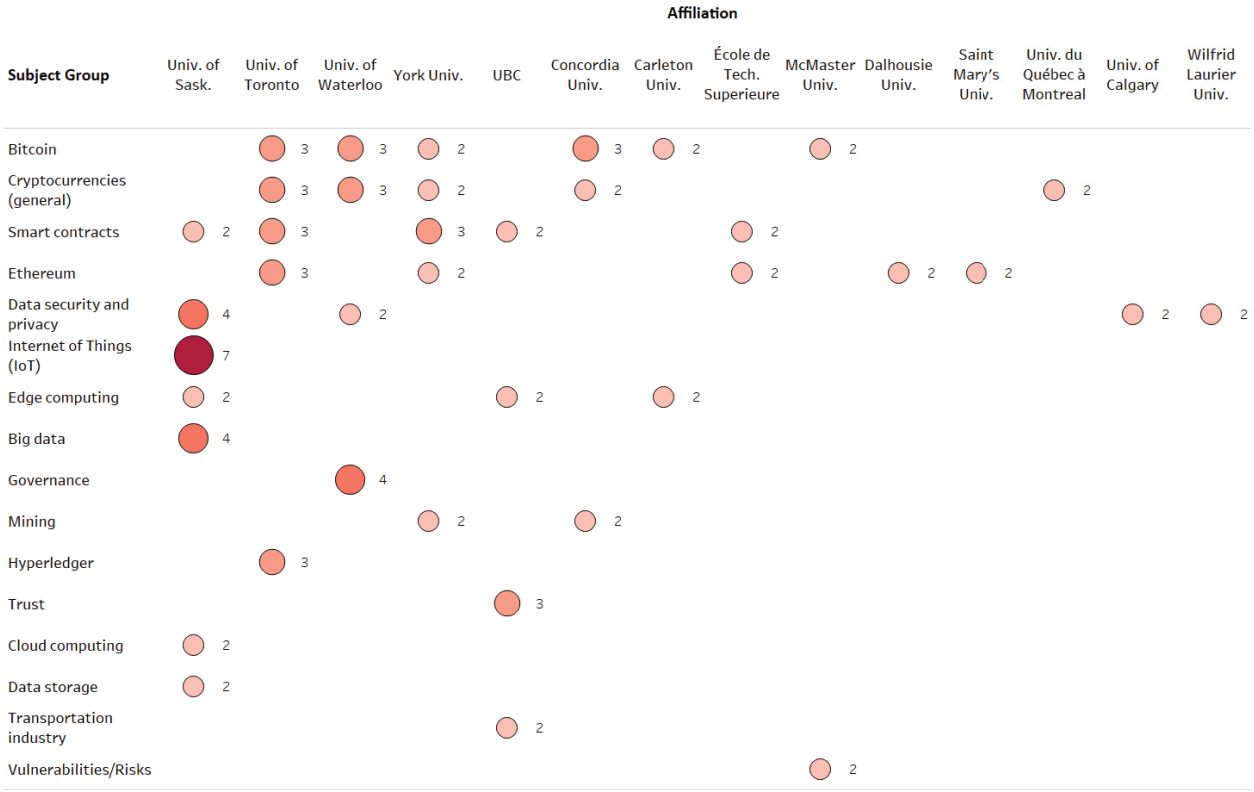

Figure 8. Canadian Organizations, Areas of Research Interest

Of the University of Saskatchewan's nine publications, seven specifically mention the *Internet of Things (IoT)*. Examples include a paper that presents the idea of using blockchain-as-a-service for IoT and evaluates the performance of a cloud and edge-hosted blockchain implementation.[28] Another publication examines the network latency and constrained interaction with sensors and actuators that current cloud-centric IoT systems introduce. The paper proposes using a process called Virtual Resources (a software-defined IoT management construct that enables multi-tenancy support and load distribution) to combat the problem.[29]

The University of Waterloo has seven publications in the set, four which are primarily concerned with blockchain governance issues, including *What are blockchains and how are they relevant to governance in the global political economy?* The paper is the introductory chapter in the book "Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance" by Waterloo's Malcolm Campbell Verduyn. The book provides insight into wider debates on the promises and perils of centralized or decentralized approaches to global blockchain governance. The latter have become critically important for policy-makers in a period in which even states and regions that have long advocated for more flexible,

decentralized governance approaches are beginning to consider shifting towards more centralized, formal governance strategies as applications of blockchain grow in size, scope, and prominence.[30]

Another Waterloo paper, *Bitcoin, crypto-coins, and global anti-money laundering governance,* assesses the effectiveness of the global anti-money laundering regime in balancing both the challenges and opportunities presented by cryptocurrencies. One of the main arguments advanced is that the threats that crypto-coins presently pose for global anti-money laundering efforts stem less from their illicit uses as digital currencies and more from issues with their underlying blockchain technologies.[31]

4.8 Areas of Research Interest—Military Author Affiliations

A similar matrix was developed to show the areas of research focus of the military affiliations (Figure 9). As in the map above, the number beside the bubble represents of the number of publications from the author affiliation containing the subject group.

	Affiliation																			
Subject Group	National University of Defense Technology, China		US Air Force Research Laboratory, USA		US Army Research Laboratory, USA		Defence Institute of Advanced Technology, Pune, India		Naval Postgraduate School, USA		Air Force General Hospital, Beijing, China		US Army Engineer R&D Center, USA	
Data security and privacy	4		5		4					1				
Consensus	5		4		2			1				1		
Cloud computing	2		7		3									
Cryptocurrencies (general)	7		2		2									1
Cryptography	4		3					1		1				
Peer-to-peer networks	4		2		1			1						
Bitcoin	6													1
Vulnerabilities/Risks	2		3		1							1		
Financial services industry	4		1		1									
Proof of stake			3		2									
Proof of work		1	3		1									
Protocols	3		1		1									
Algorithms	3		1											
Applications	3							1						
Trust	2		1		1									
Cybersecurity			1		1			1						
Military			1					1		1				
Mining		2	1											
Big data		1	1											
Crime			1		1									
Data storage			1		1									
Double spending			1		1									
Ethereum		1	1											
Identity management		1						1						
Internet of Things (IoT)		1		1										
Public Key Infrastructure		2												
Smart contracts		2												
Transportation industry		1								1				
Edge computing			1											
Fault tolerance			1											
Governance														1
Hash functions		1												
Healthcare industry												1		
Hyperledger			1											
Logistics								1						
Permissioned blockchain		1												
Scalability		1												
Transparency			1											

Figure 9. Military Affiliations, Areas of Research Interest

As Figure 9 shows, most of the 19 publications from the National University of Defense Technology of China are concerned with cryptocurrencies[32,33] (particularly bitcoin)[34,35] and issues surrounding consensus protocols.[36,37]

The US Air Force Research Laboratory (AFRL) has 11 publications in the set, with seven primarily focused on using blockchain to secure data in the cloud. Examples include:

- *Real-time index authentication for event-oriented surveillance video query using blockchain.* Information from surveillance video is essential for situational awareness. Nowadays, a prohibitively large amount of surveillance data is being generated continuously by distributed video sensors. It is very challenging to immediately identify the objects of interest or suspicious actions of individuals from thousands of video frames. Indexing the big data is critical to solving this problem. However, exchanging the index information among devices in different layers raises security concerns, as an adversary can capture or tamper with features to mislead the surveillance system. In this paper, a blockchain-enabled scheme is proposed to protect the index data through an encrypted secure channel between nodes.[38]
- *ChainFS: blockchain-secured cloud storage*. This conference paper, co-authored with ARL and Syracuse University, presents a middleware system called ChainFS which secures cloud storage services using a minimally-trusted blockchain. The system, implemented on the Ethereum platform, stores data files in the cloud and exports minimal and necessary functionalities to the blockchain for distribution and file operation logging.[39]
- *CloudPoS: a proof-of-stake consensus design for blockchain integrated cloud.* The authors propose a blockchain-based data provenance architecture (BlockCloud) that incorporates a proof-of-stake-based consensus protocol (CloudPoS) for securely recording data operations in a cloud environment. Researchers from ARL, Old Dominion University and Norfolk State University are co-authors of the paper.[40]
- *Security implications of blockchain cloud with analysis of block withholding attack.* Achieving consensus in a proof-of-work blockchain such as Bitcoin demands computational power from miners in exchange for a reward. As a result, there is an ever-present possibility that nefarious miners will try to exploit the system by augmenting their mining power. In this paper, the authors discuss blockchain's capability in providing assured data provenance in the cloud, as well as the technology's vulnerabilities. They model a block withholding (BWH) attack and show that a BWH provides rogue miners with ample resources to disrupt the efforts of honest miners.[41]

The US Army Research Laboratory (ARL) has five publications in the set, all produced in collaboration with the AFRL. In addition to the papers mentioned above, the two organizations have cooperated on addressing the issue of countering the double-spending problem in next-generation blockchains;[42] they also discuss consensus protocols for blockchain-based data provenance.[43] ARL and AFRL have also published a paper with Howard University entitled *IShare: blockchain-based privacy-aware multi-agent information sharing games for cybersecurity*, which discusses the design, development, and evaluation of a novel blockchain-based information sharing framework for cybersecurity. In the proposed framework, the decentralized nature of the blockchain, combined with digitally-signed transactions, ensure that an adversary cannot pose as a legitimate organization/user and cannot control or alter the system.[44]

The single paper in the set from India's Defence Institute of Advanced Technology, *Employability of blockchain technology in defence applications*, examines the viability of using blockchain to ensure the

integrity and provenance of data in networked military operations (and maintaining sustainability of these networks). Three case studies are analyzed for the feasibility of incorporating blockchain technology into the existing Network Enabled Military Operations (NEMO) framework. The case studies highlight blockchain properties such as immutability, fault tolerance, trust, data provenance and transparency.[1]

The paper from Canada's Defence Research and Development Canada (DRDC), published in April 2018, explores a range of possible blockchain applications in tactical networks, including supply chain management, network management and data security.[45]

4.9 Research Momentum

As shown above, the grouping, categorizing and ranking of related publications, combined with the creation of keyword co-occurrence maps, can provide some insight into the quantity and focus of activity within a domain of research and that of the key players. They do not, however, sufficiently convey the *momentum* of a topic relative to other subjects in the same set of data over the same period of time. In other words, the quantity of records in a group does not necessarily suggest which topics are "hot", which are well-established, and which are emerging.

In order to better understand the relative research momentum of research topics over the past five years, the subject groups were plotted using an R&D momentum indicator (Figure 10). Further explanation of the methodology behind the indicator is included in the Appendix, but essentially it plots the standard deviation of standardized measures of publication counts and velocity (the rate of publication increase) on two axes. Nodes which plot to the left of the Y-axis intersection have below-average velocity and those found below the X-axis have relatively smaller publication counts. A third dimension is added by sizing nodes relative to the total number of underlying publications. Even a small node which plots to the right/lower side of the axes may be of interest, since emerging topics are typically small in numbers as they begin to attract research attention and increase in velocity.

The four quadrants are defined as such:

1. **Established Topics** (top left): contains groups with a high number of publications but low acceleration over the past five years.
2. **Hot Topics** (top right): groups with a high number of publications and high acceleration.
3. **Emerging Topics** (bottom right): groups with a low number of publications but high acceleration
4. **Brand New Topics**[i] (bottom left): groups with a low number of publications and low acceleration.

[i] Typically this quadrant can contain topics that demonstrate declining research interest as well as "brand new" topics. However, given that 91% of the dataset consists of publications from the past three years alone (2016-2018), all subject groups in this quadrant can be considered "brand new" in the context of this analysis.

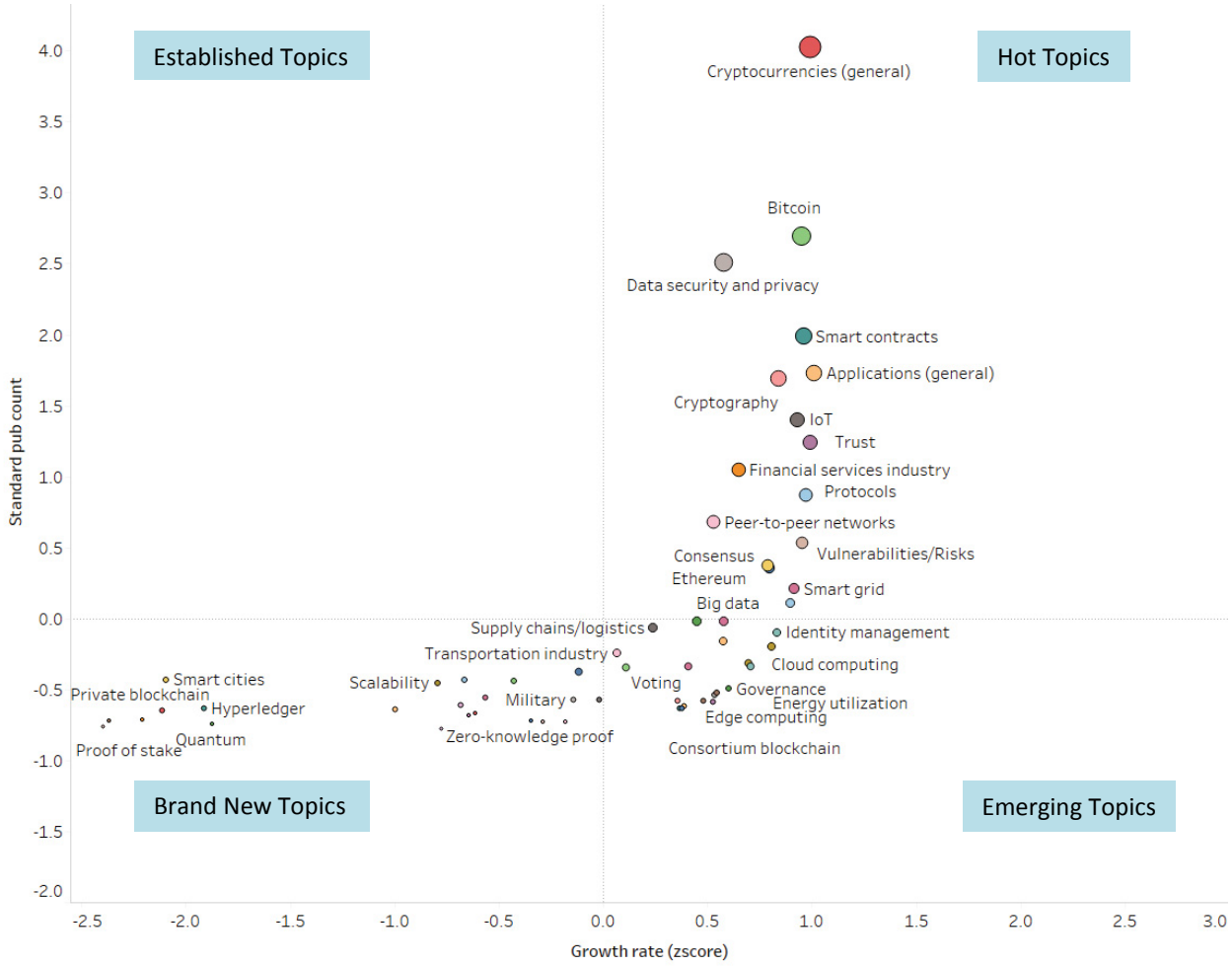

Figure 10. Research Momentum, Literature Subject Groups

Perhaps not surprisingly, especially considering the fact that much of the research in DLT is very new, there are no subject groups appearing in the *Established Topics* quadrant.

Due to the large number of subject groups, not all nodes and their labels can be shown clearly on the full graph in Figure 10. Therefore, Figures 11 to 13 below are expanded versions of each of the three quadrants containing groups.

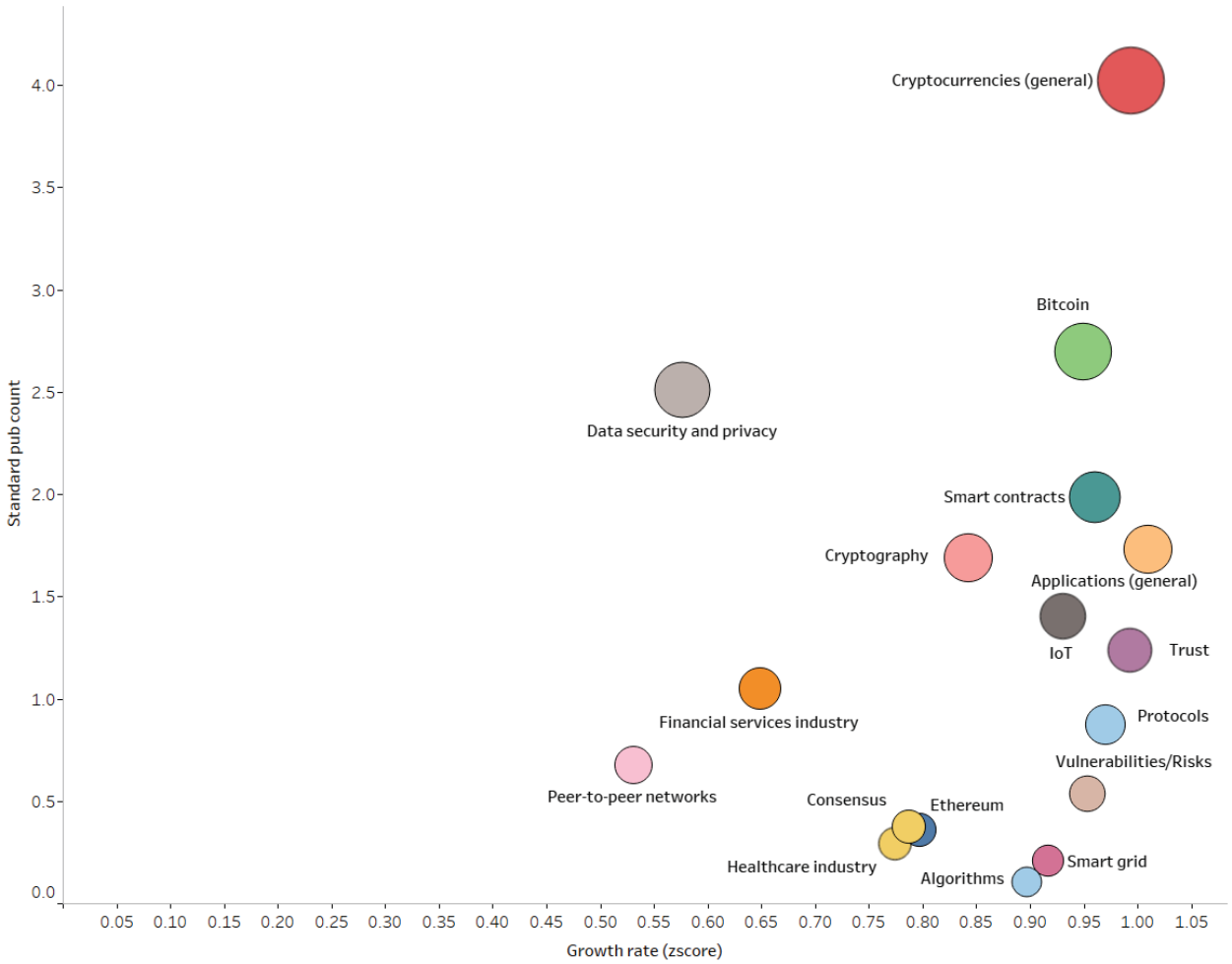

Figure 11. Research Momentum, Hot Topics Quadrant

The *Hot Topics* quadrant (Figure 11) contains several of the largest subjects in the dataset (shown earlier in Figure 9), including *Cryptocurrencies (general), Bitcoin, Smart contracts* and *Data Security and privacy*. The *Financial services industry* group also appears here, although displaying less acceleration than other industry/application groups such as *Healthcare industry* and *Smart grid*, an indication of the swelling research interest in additional uses for blockchain beyond electronic money.

The groups *Trust, Protocols* and *Vulnerabilities/Risks* are three of the highest accelerating groups in the quadrant, suggesting an increasing research focus on examining the underlying features of DLT and in resolving the fundamental weaknesses and liabilities of the technology.

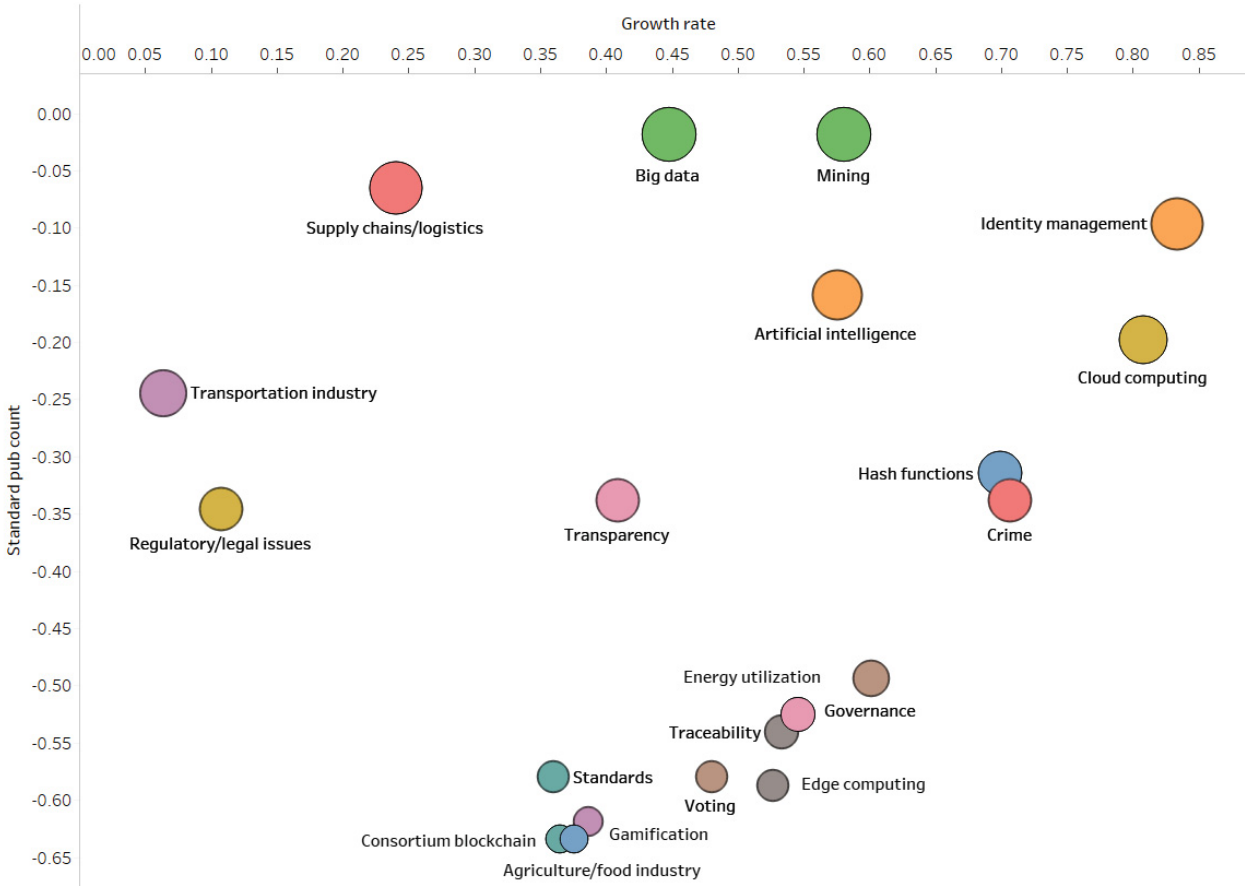

Figure 12. Research Momentum, Emerging Topics Quadrant

As mentioned, *Emerging Topics* are those subject groups containing a low number of publications but demonstrating high acceleration over the time frame. The fastest-moving topic in the quadrant (Figure 12) is *Identity management*, a subject which is of particular interest to military and government organizations. Several of the publications in the group will be described in sections 4.9.1 and 4.9.2. Others include:

- *Biometrics on the blockchain*. This paper examines the benefits blockchain offers to biometric systems developers and users, and how biometrics can be integrated into DLT systems to achieve better security, scalability and privacy.[46]
- *A first look at identity management schemes on the blockchain*. Researchers at OneSpan Corp in the US evaluate three DLT-based identity management systems - uPort, ShoCard, and Sovrin.[47]
- *A blockchain ecosystem for digital Identity: improving service delivery in Canada's public and private sectors*. The author identifies two areas in Canada that stand to benefit the most from blockchain—government services and healthcare. Blockchain could reduce government costs associated with physical office space, verification, call centres and more. Blockchain could also transform healthcare by streamlining patient administration and engaging consumers in self-care and health management at home. Patients and providers could securely identify during appointment bookings, access records and authorize a "circle of care" to share their patient history across multiple providers and family members.[48]

- *Who am I? Secure identity registration on distributed ledgers*. Researchers from University College London, UK, address the question of how to register identities and attributes in a system built on globally visible ledgers. They propose a variety of possible solutions and analyze the tradeoffs among privacy, usability and integrity. They present an implementation of one of their solutions using Ethereum.[49]

Also appearing in the *Emerging Topics* quadrant are groups that will be explored in greater detail in the upcoming sections, such as *Regulatory/legal issues*, *Supply chains* and *Governance*. Cloud computing is also a quickly emerging topic and, as shown earlier, is a central theme in a number of the publications from the US Air Force Research Laboratory.

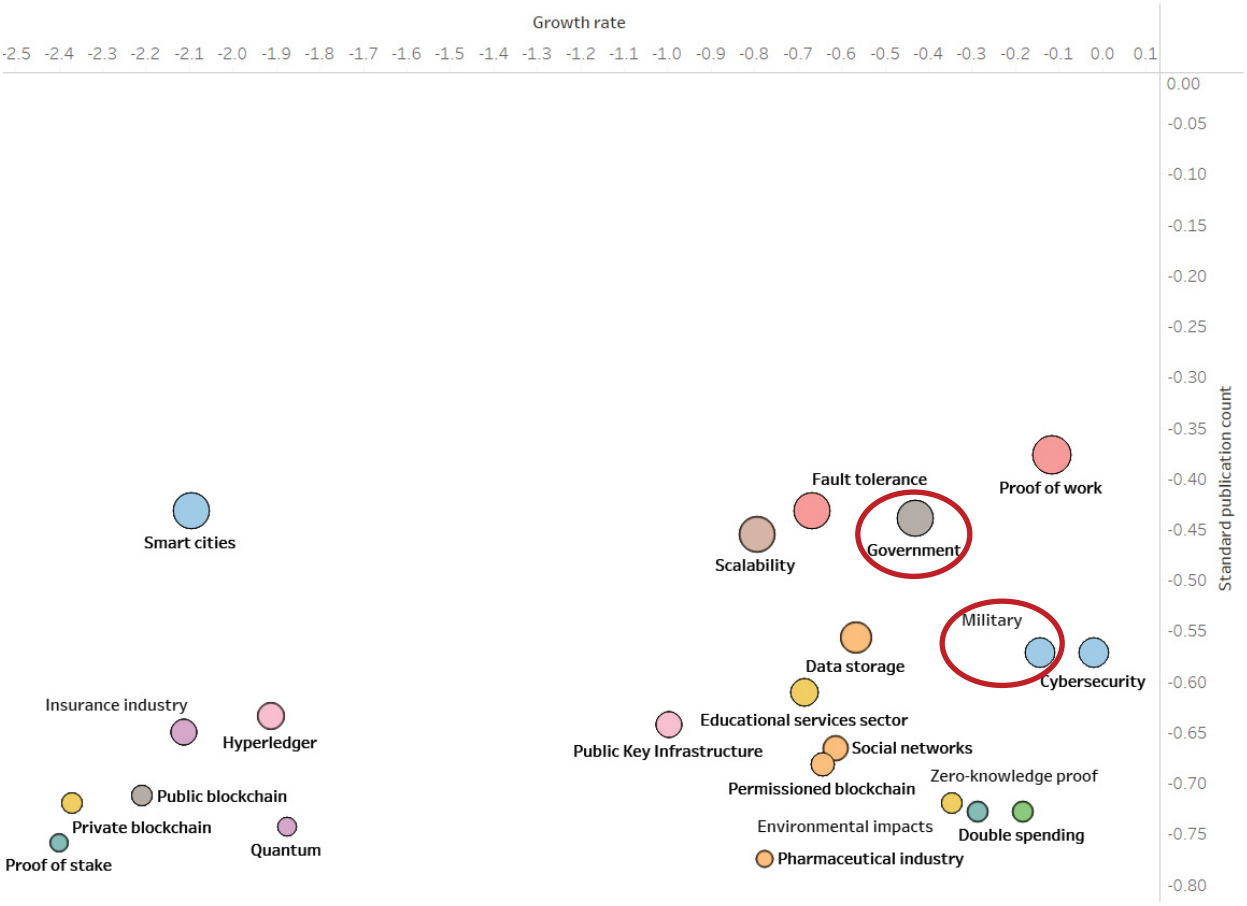

Figure 13. Research Momentum, Brand New Topics Quadrant

The *Brand New Topics* quadrant contains the *Military* and *Government* subject groups (circled in red in Figure 13). These are examined in more detail below.

4.9.1 Military Applications

The *Military* subject group is comprised of 36 publications that contain one or more military-related keywords.[j] The majority of the papers are concerned with topics such as data security, communications, supply chains and identity management.

Military operations are supported by networks that permit the generation, transmission, collection, analysis and exploitation of data to enable better decision making, while at the same time interfering with the adversary's ability to do so (also known as "datafighting").[50] It is of utmost importance to guarantee a high level of data integrity, confidentiality and availability and to ensure its sustainability in hostile environments. *Blockchains in national defense: trustworthy systems in a trustless world* proposes that blockchain technology offers three significant advantages over traditional cyber defense strategies:

- First, rather than trying to defend boundaries from compromise, blockchains assume that networks will be compromised by both adversaries and trusted insiders. They are designed to defend data in a contested cyber environment.
- Second, blockchain networks harness the aggregate power of the network to actively resist the efforts of malicious actors. That is, blockchains take advantage of the asymmetry of many against few.
- Lastly, the security that blockchains provide is not dependent on secrets or trust. There are no passwords to be exposed, cryptographic keys to be protected, or administrators to be trusted. Blockchains provide an inherent security function on which additional security functions can be added, depending on the application.[50]

As result of these advantages, blockchains are capable of operating successfully and securely on the open internet, without a trusted central authority, and while fully exposed to hostile actors. Given their ability to protect the integrity of data in spite of adversary actions, blockchains offer significant military utility in the highly contested environments of the future.[50]

The globalization of manufacturing supply chains presents a security concern for many nations, as the electronic hardware embedded in the technology used for public safety and defence is increasingly assembled or produced in other countries. One estimate indicates that, in the US alone, as many as fifteen percent of all spare and replacement parts purchased by the Pentagon are counterfeit.[51] As noted in *Leveraging blockchain technology to protect the national security industrial base,* an emerging national security challenge related to international supply chains are attacks in which substandard, counterfeit, or maliciously-modified electronic components are introduced into the hardware on which the national security industrial base operates. Distributed ledger technology presents an opportunity to transform supply chain transactional data in order to make it easier to ascertain the provenance of equipment used in the protection of national security.[52] Every circuit board, processor, and software component from "cradle to cockpit" could be tracked—the circuit board design firm could use blockchains to record every iteration of a circuit. Manufacturers could record the model and serial number of every item produced. Finally, distributors could log the sale of circuits to system integrators, who could record the allocation of circuits to specific aircraft assemblies, and so on.[50]

Lockheed Martin, the first US military contractor to implement distributed ledger technology, has been working with Guardtime Federal to incorporate blockchain into their own supply chain processes.[42] As

[j] Such as *army, navy, air force, military, national security, defense, battlefield, tactical, combat,* etc.

Lockheed is also the producer of the Aegis Combat System used in the naval ships belonging to several countries, there has recently been speculation that blockchain is the future of battleship control systems. For example, by utilizing blockchain's ability to verify that all nodes are working from the same set of data, the system could potentially coordinate weapon control to neutralize threats.[53,54]

Two publications in the set examine the threat posed by "fake news" to national security (such as manipulation of elections or misleading public perception) and how blockchain could be a solution. According to an MIT study, Twitter users are 70% more likely to retweet falsehoods than true facts.[55] Simply put, fake news spreads quicker and reaches a wider audience than the truth. In *Fake news: a technological approach to proving the origins of content using blockchains*, the authors present a blockchain-based application that is capable of determining the provenance of any source of digital media, including images used out of context in attempts to mislead.[56]

A thesis from the Naval Postgraduate School titled *Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security* shows how information, whether true or false, can be spread rapidly online due to the accessibility and interconnectedness of the Internet ecosystem. Blockchain could help eradicate fake news through the use of digital identities and a verifiable reputation system.[57]

Blockchain also has potential application to border control and immigration. A publication from India's National Institute of Technology proposes using blockchain to create secure and scalable departure and arrival records of passengers. Their framework uses Hyperledger Fabric to maintain records of entry and exit, and addresses concerns about storage of biometric data. The researchers also explore the possibility of modifying existing border kiosks to work with the blockchain architecture at the back-end, so that passengers are not required to become familiar with a new procedure.[58]

Trials, Pilot Projects and Funding Solicitations

There are a number of other initiatives recently announced or just underway that are too new to have had any results published in the scholarly literature. These include several pilot projects and trials, as well as recent solicitations for blockchain R&D from various government agencies. For example, the US National Defense Authorization Act for fiscal year 2018 includes a provision ordering the Department of Defense (DoD) to conduct a comprehensive study of blockchain, particularly with regard to cybersecurity. Meanwhile, some DoD departments and agencies have been exploring blockchain on their own, such as a way to deliver secure messaging to deployed troops, and how to protect the digital 3D printing supply chain for ships at sea or units in the field.[59]

The US **Defense Advanced Research Projects Agency (DARPA)** is currently funding efforts to discover if blockchains could help protect highly sensitive data, with potential applications for everything from nuclear weapons to military satellites. The growing complexity of modern systems, including weapon systems, is such that vulnerabilities are both more likely and less detectable. With DLT, instead of searching for vulnerabilities, which is equivalent to searching for a needle in a haystack, it would be theoretically possible to monitor every stalk of hay, every digital asset that constitutes the system you want to protect.[60] The idea is not so much to try to stop intruders from hacking into a database, but to know where they have gone and what they have done once they are in.[61-63]

Secure messaging is another focus of DARPA, since it is critically important that soldiers on the ground are able to communicate securely with headquarters. In the past, it has been difficult for the military to

accurately assess when communication channels or systems have been compromised. By decentralizing significant portions of the DoD back office, validated data can be sent much faster, thereby reducing exposure to hackers and extended data transmission delays. According to their SBIR solicitation,[k] DARPA seeks a "secure messaging and transaction platform accessible via a web browser or standalone native application." One platform requirement is that it must utilize an existing blockchain technology such as Ethereum. Additionally, the application must be scalable and undergo commercial testing.[63] To date, the contracts awarded under the project are:

- SIMBA: Secure Messaging on the Blockchain Architecture [Indiana Tool & Mfg]
- Secure Messaging Platform : Addressable Encrypted Blockchain (AEB) [BDPK Ltd.]
- Secure Messaging Platform [Stealth Software Technologies]
- Secure Information Exchange Platform [SynaptiCAD Sales Inc.]
- Secure Messaging Platform [CipherTrace Inc.]
- Secure Messaging Platform [Metronome Software]
- Secure Messaging Platform (SMP) as a Service (SMPaaS) [Harmonia Holdings Group LLC]
- Secure Messaging Platform [WICKR Inc.]

The US Department of Defense Joint Staff, J4 Logistics Directorate and the Deputy Assistant Secretary of Defense for Maintenance, Policy, and Programs are co-leading a project to create a "point of use, time of need" digital supply chain enabled by Additive Manufacturing (AM) and blockchain. The digital nature of AM means that parts and products are easier to share and transmit, enabling the creation of a digital supply network and supply chains. However, AM, with its reliance on the digital thread, is one area which can be especially vulnerable to cyber threats and intrusions. In order to fully realize the benefits of AM within a defined distribution network, secure data transport needs to be addressed, and blockchain is foreseen as a potential solution to mitigate those risks.[64] Other participants in the project include the Dept. of Commerce, National Institute for Standards and Technology, National Center for Manufacturing Sciences, Commercial Technologies for Maintenance Activities, the US Navy, US Army, US Marine Corps, US Air Force, the Defense Logistics Agency and industry partners.

Mentioned in the US Defense-wide **Research, Development, Testing and Evaluation (RDT&E) request to Congress for fiscal year 2019** is a project called Blockdata, which involved an assessment of various blockchain technologies to support data integrity for distributed sensors and their processed data sets. The project evaluated various blockchain technologies currently being developed in the commercial sector and explored their applicability, performance and adaptability for joint warfighter applications. The project identified initial application areas and then transitioned to a classified DoD agency.[65]

The objective of the **US DoD Defense Logistics Agency's** SBIR solicitation *Sharing of Defense Research, Development, Testing, and Evaluation (RDT&E) Data Distribution using Distributed Ledger Technologies* is to develop a capability for efficiently and verifiably sharing documents and scientific data sets using DLT, and to demonstrate how such capability can be integrated with repositories implemented using conventional technologies such as XML databases. The project will be carried out in three phases:

[k] The Small Business Innovation Research (SBIR) program is a competitive funding program that encourages domestic small businesses to engage in Federal Research/Research and Development (R/R&D) that has the potential for commercialization.

1. Design and demonstration of an efficient and verifiable document and scientific data sharing solution using open source blockchain platforms. The design should address the nature of the proposed blockchain solutions, e.g. a permissioned blockchain vs an open blockchain.
2. Demonstration of the capability of the prototype using a set of documents and scientific data provided by the Defense Technical Information Center (DTIC).
3. The resulting system should enable increased information sharing, with both military and commercial applicability.[66]

The **US Navy** has a number of initiatives underway:

- *Clearinghouse for Subsistence Ordering & Receipt (CSOR).* The Navy wants to develop an information system that will provide Subsistence Total Order and Receipt Electronic System (STORES) operators and Combat Logistics Officers with a Financial Improvement and Audit Readiness (FIAR)-compliant "clearinghouse" for food subsistence orders. The current Navy process for ordering operational forces subsistence items is cumbersome and causes duplication of work. Also, ships do not always have up to date vendor catalogs. These conditions contribute to "late" orders and can create a financial obligation gap resulting in a FIAR non-compliance issue. The new system will work across a wide range of business logistics applications (ordering, receipt processing and inventory management) and utilize blockchain technology to support electronic reconciliation of financial transactions.[67]
- *Using blockchain to secure naval manufacturing*. The U.S. Navy has plans to trial blockchain technology to bring added security to its manufacturing systems, particularly additive manufacturing (3-D printing). It wants to securely share data throughout the manufacturing process as it creates critical equipment for deployed forces. Led by the Naval Innovation Advisory Council, the trial will use blockchain technology to create a data-sharing layer between the Navy's various 3-D printing sites.[68,69]
- *Navy approved multi-factor authentication (MFA) for personal mobile devices.* The objective is to design and develop a software-based MFA mobile device based on blockchain technology and define a draft set of standards by which MFA solutions will be evaluated and accredited by the Navy Approving Official.[70]
- *NAVAIR and ITAMCO to develop a parts-tracking blockchain*. The Naval Air Systems Command (NAVAIR), in partnership with Indiana Technology and Manufacturing Companies (ITAMCO), is exploring the use of blockchain to help track aviation parts throughout the parts life-cycle. Knowing the origin and history of flight-critical aircraft parts is a resource-consuming process that drives up the cost to operate military aircraft. Currently, once parts are delivered to the user, they are tracked with pen and paper on a Scheduled Removal Component Card and manually entered into a database. The new model will be a permissioned blockchain with a consensus mechanism requiring less computing power than the proof-of-work mining method utilized in the bitcoin blockchain.[71]

The **US DoD Special Operations Command (SOCOM)** has an SBIR solicitation titled *Automated Processing, Exploitation and Dissemination*. The objective is to develop software that executes on aircraft near real-time level 1 processing, exploitation, and dissemination (PED) of full motion video, signals intelligence/electronic warfare, synthetic aperture radar, and other sensors and disseminates these products over tactical data links with the end state of reduced PED personnel. Research and development efforts are to include the use of blockchain to share tactical information across airborne platforms so that all systems and sensors are not duplicating product development, and that the databases automatically query all platforms for data prior to the software creating a product.[72]

The goal of the **US DoD Defense Microelectronics Activity** project, *Blockchain Supply Chain Enhancement for Trusted & Assured FPGAs and ASICs*, is to develop an affordable and highly secure Supply Chain Risk Management (SCRM) system enhanced by blockchain technology. Trusted and assured microelectronics supply chains are globally distributed and offer many opportunities for supply chain compromise by adversaries. An opportunity exists to establish a cryptographically secure supply chain that utilizes advanced technology. This technology can be implemented through Physically Unclonable Functions (PUFs) and will allow each device to be uniquely identified through the use of unique cryptographic keys. With this implementation, device manufacturing information will be maintained securely within each device, allowing device supply chain interrogation at any time. Blockchain-enhanced SCRM flow would be implemented by the use and integration of calendar blockchain technology that would create an immutable audit trail for each field-programmable gate array (FPGA) device from its design and fabrication through user bitstream configuration and field updates.[73]

The **US Department of Homeland Security (DHS)** has the following projects underway or in development:

- *Blockchain applications for homeland security missions.*[74] In November 2016 DHS released a solicitation through SBIR with the objective of designing and prototyping an ecosystem that applies blockchain technology to significantly improve DHS analytics, missions, and operations. Possible use cases included, but were not limited to, crypto-certified transactions involving users and devices for the Internet of Things applications (IoT) such as encrypted data transactions and analytics for first responders; information sharing and analysis between state, local, and federal law enforcement; and third parties' involvement, perhaps in applications that improve security and experiences for the traveling public, or that improve bio-threat awareness. A contract was awarded to Blockcypher Inc.: Blockchain Platform for Multiple Blockchains, Applications, and Analytics Phase II.
- *Decentralized key management using blockchain*.[75] The objective of this SBIR Proposal is to conduct the research needed to enable blockchain technology to serve as a decentralized foundation for privacy-respecting identity management. Contracts awarded so far include:
    - Verifiable Claims and Fit-for-Purpose Decentralized Ledgers [Digital Bazaar Inc.]
    - Applying Blockchain to Decentralized Identity [Respect Network Corp.]
    - Decentralized Key Management using Blockchain [Respect Network Corp.]

The **DHS's Science and Technology Directorate (S&T)** is also leading proof-of-concept deployments on behalf of the U.S. Border Patrol to evaluate how blockchain can ensure imagery and sensor data from its cameras are authentic and unaltered. This would make the spoofing of a device much more difficult, meaning a criminal could not hijack a security camera and loop the footage. Not only would the blockchain know if a security camera is legitimate, it would also prevent tampering with any footage or captured data from a secured device.[76] The technology was demonstrated recently by S&T and Factom at IoT World. S&T is also partnering with the U.S. Customs and Border Protection to explore how it can use blockchain and distributed ledger technologies for its mission areas, such as facilitating international passenger travel and enhancing shipping, logistics and customs.[77]

In September 2018 the **US National Science Foundation (NSF)** issued an SBIR proposal "covering a wide range of technology areas of current and emerging commercial significance and impact spanning all areas of distributed ledger including blockchains, Directed Acyclic Graphs (DAGs)[I], and related capabilities (cryptography, smart contracts etc.)". Projects should address "pain point" areas such as enhancements to speed, scalability, efficiency, improved functionalities/capabilities, enhanced security, consensus, immutability, information and identity validation, trusted data/inputs, digital privacy, artificial intelligence (AI) applications, IoT integration, autonomous systems / economies, and improvements to enhance user adoption.[78] The solicitation closes December 4th, 2018.

In the **United Kingdom**, the **Defence Science and Technology Laboratory (DSTL)** has partnered with the University of Warwick and Crossword Cybersecurity to explore novel uses of blockchain-enabled documents in military environments. The project will look at how to provide access to sensitive information in a range of environments, including harsh operational theatres. Crossword also subcontracted Simplexity Analysis to assist in the conceptual design stages.[79]

Cambridge Consultants, a UK-based consultancy, has also worked with DSTL on using a blockchain to improve the trustworthiness of a network of sensors on, for example, security cameras.[80]

The **UK Ministry of Defence (MoD)** has enlisted Thales and Accenture to work on a proof of concept for using blockchain to help secure aerospace and defence supply chains. The companies have created two mechanisms to identify material in the supply chain: programmable unique functions, which are used to assign a "fingerprint" to small components like microchips; and "cryptoseals," which are physical seals placed around bags of products such as diodes. When a seal is tampered with outside of the approved process, it communicates to the blockchain using the Internet. The companies believe the technology will have uses for the military, as well as their own internal programs which they use to deliver solutions to the MoD.[81]

In **Russia**, the Russian Ministry of Defense is launching a research lab to analyze how blockchain technology can be used to mitigate cybersecurity attacks and protect critical infrastructure. One of the priorities of the nation's military technology accelerator (known as the ERA) is the development of an intelligent system to detect and prevent cyberattacks on important databases. The lab, which is being built in the Russian coastal town of Anapa, will ultimately fall under the General Staff of the Armed Forces of the Russian Federation's Eighth Directorate, which focuses on information security.[82]

The Russian telecommunications company Voentelecom, which provides communication and integration services to federal executive authorities and the Ministry of Defense in Russia, is also considering possible applications for blockchain in the Russian military.[83,84]

Clearly, distributed ledger technology is attracting a significant amount of interest from military organizations around the world. However, notwithstanding the recent escalation in R&D and pilot projects, it is not yet clear if DLT will provide any real added-value (versus traditional database technologies) in the long term. The official magazine of the European Defence Agency, for example, estimates that the benefits and real application of blockchain in the fields of military communications and countering cyber threats will likely not be seen until 2025 at the earliest.[85]

[I] For more information on the differences between DAGs and blockchains see https://tinyurl.com/yd9vdnv3.

4.9.2 Government Applications

The *Government* subject group contains a total of 53 publications, all published between 2016 and 2018 (Figure 14), indicative of its appearance in the *Brand New Topics* quadrant in the research momentum indicator (Figure 13 above).

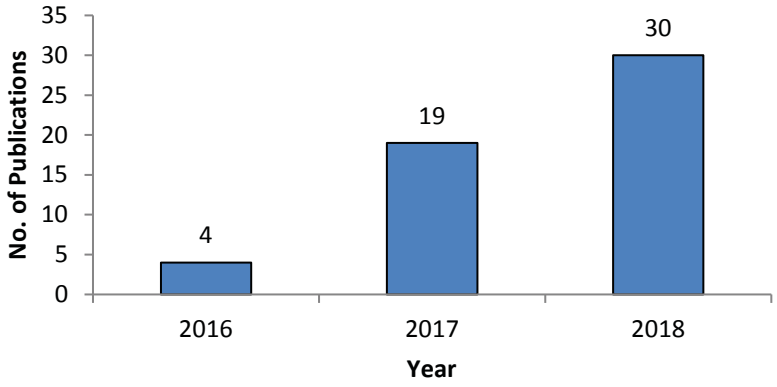

Figure 14. Temporal Distribution, Government Publications

Several of the documents in the group examine the implications of bitcoin and other cryptocurrencies on government processes and monetary policies, while others are focused on data security and regulatory/legal issues. Overall, the potential range of DLT applications in government appears almost infinite. Some of the use cases include:

- Combatting voter fraud[86-88]
- National identity management and corporate registers, such as Estonia's e-Residency program,[89-92] Canada's registry for cross-border travel[45] and Microsoft/Accenture's initiative for refugee identity systems[93]
- Smart contracts, procurement, and tendering[45,91,94-96]
- Food and drug traceability and drug anti-counterfeiting[97-99]
- Health surveillance and tracking of opioid abuse[100,101]
- Security of critical data assets, for example Estonia's Keyless Signature Infrastructure[86,91,94]
- Digital property ownership[94]
- Smart city management[102-104]
- Smart grid and other energy management/security applications[105]
- IoT and other cyber-physical security[45,106-108]
- Anti-counterfeiting, protection of digital manufacturing and parts management[53,109-111]
- Privacy preservation and sharing of health records (see the US Federal Drug Administration's proof of concept projects, and the EU-funded project entitled My Health, My Data[91,92,106,112,113]
- Issuance of government bonds (trials are underway in Austria, Australia and Thailand)[114]

As illustrated in a map from the Organisation for Economic Co-operation and Development, based on data collected by the Illinois Blockchain Initiative[m]), there are currently over 200 government DLT projects in 45 countries around the world, and the number is growing rapidly.[115]

[m] See https://illinoisblockchain.tech/ and http://bit.ly/blockchain-govt-tracker

In the **United States**, the strong interest from many federal departments in distributed ledger technology prompted the US General Services Administration (GSA), through its Emerging Citizen Technology Office, to launch the U.S. Federal Blockchain Program for federal agencies and U.S. businesses interested in implementing DLT within government.[81] The GSA recognized that government agencies across the US are eager to implement the technology as a solution to unresolved issues. However, a centralised platform within government was missing to share best practices, make sense of use cases and go forward with the technology in a more judicious approach.

To that end, the GSA hosted the first U.S. Federal Blockchain Forum on July 18, 2017, uniting more than 100 federal managers from dozens of agencies to discuss use cases, limitations, and solutions. Agency teams submitted over 200 potential use cases for blockchain technology. Tellingly, a study of the use cases showed that blockchain may not be the appropriate solution to all the problems that an agency is facing.[96,115,116]

In **Canada**, on March 22, 2018, the Institute on Governance hosted a Blockchain in Government Workshop, an event that brought together public servants and stakeholders from private industry who are interested in the applicability and benefits of blockchain technology within the Canadian government. The workshop report summarizes the content and highlights the common themes and issue areas that arose during each session.[117]

In January 2018, the National Research Council of Canada, through its Industrial Research Assistance Program (NRC IRAP), successfully launched the Government of Canada's first-ever live trial of public blockchain technology (on Ethereum) for the transparent administration of government contracts.[118] The program began proactively publishing information on new and amended Contribution Agreements with firms in real time. Since the launch, NRC IRAP has been exploring ways to expand its experiment with blockchain and reliably share data with the public. The program is now hosting its blockchain explorer application, developed by Bitaccess, on the InterPlanetary File System (IPFS).[119]

The Bank of Canada is also involved in a number of projects involving DLT:[120]

- Project Jasper was a collaborative research initiative between the public and private sectors to understand how DLT could transform the wholesale payments system. The project was recently completed, with the conclusion that DLT is not yet sufficiently mature to run a national interbank payment settlement system.[54]
- The Bank has partnered with Payments Canada and the TMX Group to investigate a DLT solution for a securities settlement system using central bank money.
- The Bank and Payments Canada have partnered with the Monetary Authority of Singapore and the Bank of England to work on a cross-border, cross-currency settlement system. This collaboration combines Project Jasper and Singapore's Project Ubin, with a view to using DLT to make cross-border payments faster and at lower cost.
- The Bank is a partner of the MIT Media Lab in their Digital Fiat Currency project, as well as a founding member of the Blockchain Research Institute.

The Canada Revenue Agency (CRA) is looking into cryptocurrencies and the risks they pose to the Canadian tax base, in order to inform future risk assessment and audit approaches, in addition to developing the means for detecting tax non-compliance. The Agency is also looking to build a new blockchain-based digital identity service, expanding on SecureKey Concierge's service, which is used by

individuals to authenticate themselves to the federal government through the banking sector.[54]

IBM Canada, the Province of British Columbia, and the Digital ID & Authentication Council of Canada (DIACC) collaborated to develop a proof-of-concept to explore the viability of blockchain technology as a tool for more secure, effective, and efficient corporate registrations—both within a single province and across multiple jurisdictions. Further work on the proof-of-concept is required to strengthen its viability.[91,121]

Several other federal government departments including Elections Canada, Innovation Science and Economic Development Canada, Treasury Board Secretariat, Communications Security Establishment, Natural Resources Canada and Public Safety Canada are monitoring developments in distributed ledger technology and/or are in the early stages of developing trials.[91]

In **Europe**, the European Union Intellectual Property Office (EUIPO) is investigating how blockchain could combat counterfeiting, which costs the EU €60 billion each year, according to the agency's research. In June 2018, the EUIPO and the European Commission organised a "Blockathon" competition in Brussels, where 11 teams of coders created a series of anti-counterfeiting blockchain solutions, drawing on support from specialists in law, IP and anti-counterfeiting. The team that won the overall prize created a "virtual twin" that cannot be copied and is sent to consumers for verification before they receive the connected physical product, which is registered on a blockchain.[122]

One of the first countries in the world to investigate distributed ledger technology was the small Baltic nation **Estonia,** which began testing DLT in 2008, before Satoshi Nakamoto's white paper had been published. Estonia dubbed the technology "hash-linked time-stamping" at the time.[123] Blockchain provides the backbone of the renowned e-Estonia program[n], which connects government services in a single digital platform. The project integrates a large quantity of sensitive data from the judiciary, legislature, healthcare, security and commercial code registries, which are stored on a blockchain ledger to protect them from corruption and misuse.[122]

Estonia went on to develop, in partnership with Guardtime Federal, a blockchain technology called Keyless Signature Infrastructure, or KSI, which secures Estonia's networks, systems and data. The KSI system provides a formally verifiable security system for the government that can function even under constant cyber-attack, and is now available in more than 180 countries.[122,124]

In the **United Kingdom**, the Food Standards Agency (FSA) completed a pilot in July 2018 using blockchain to track the distribution of meat in a cattle slaughterhouse. The FSA claimed the trial marked the first time that distributed ledger technology has been used as a regulatory tool to ensure compliance in the food sector. A number of other government departments in the UK are also exploring the technology, including the Department for Environment, Food & Rural Affairs, which is looking into how it could enhance food traceability. Her Majesty's Land Registry is investigating if it could improve the land registration and property buying/selling process using the technology, and the Department of Work and Pensions is assessing if it could help benefit claimants to manage their money.[122]

At the recent Blockchain Live conference held in London, the British Minister for Digital and the Creative Industries promised further trials and committed to invest over £10 million through Innovate UK and

[n] For more information see https://e-estonia.com.

other research councils to support blockchain projects in diverse areas like energy, voting systems and charitable giving.[125]

In the **United Arab Emirates**, *Smart Dubai* is a government and city-led initiative to make Dubai the "smartest and happiest" city in the world. As of September 2018, the government's payment portal, called DubaiPay, now uses blockchain technology for real-time reconciliation and settlement of transactions. This is another step towards Dubai's goal of becoming the world's first blockchain-powered government by 2020.[126,127] Dubai is currently working on a total of 20 use cases for blockchain to complement its existing government operations, and has strategic partnerships with IBM and Consensys to help them further their goals.[128]

In **China**, president Xi Jinping heralded blockchain as part of the "new industrial revolution" in a May 2018 speech at the Chinese Academy of Sciences. Officials and entities across private industry, the national government, local government and academia are all focused on projects related to blockchain development. Examples include:

- E-government is considered an important component of the national digitalization strategy in China, and the use of blockchain technology in e-government systems is considered a key component of the strategy.[129,130]
- The Chinese Communist Party website released a primer on blockchain technology that included discussion points on its key features, use cases, and challenges.[107]
- China's Supreme People's Court released new rules stating that blockchain technology is an approved method for storing and authenticating digital evidence.[131]
- Despite its tough stand on cryptocurrencies (bitcoin trading is banned in the country), the People's Bank of China has filed 41 blockchain patents. Moreover, Chinese companies occupy six of the top ten spots in DLT patent rankings, with Alibaba filing 90 patents. Cumulatively, Alibaba, Ten Cent and other companies have filed twice the number of patents as their US counterparts.[132]
- The Bank of China is also hoping to utilize blockchain to overhaul their cloud-based poverty reduction system. The goal is to improve outreach efforts to poor citizens in the autonomous region of Tibet. If the effort is successful, the Bank hopes the same model could be replicated in other poor areas like Gansu and Yunan.[133]
- Tsinghua University in Beijing is teaming up with IBM and Walmart to use the Hyperledger blockchain platform to digitally track the movement of pork in China. The system is designed to provide a way to indelibly record a list of transactions indicating how meat has flowed through a commercial network, from producers to processors to distributors to grocers and, finally, to consumers.[134]
- China's central government has drafted a new regulation that would strip blockchains of their anonymity, requiring users to provide their real names and national ID card numbers when registering for a blockchain service. The policy may place significant restrictions on ongoing blockchain development. At the end of October 2018, the Cyberspace Administration of China, the country's internet regulator, released a draft of the policy, which would also require blockchain services to remove "illegal information" quickly before it spreads among users. The services will also be required to retain backups of user data for six months and provide them to law enforcement whenever necessary.[135]

Although there is a significant amount of activity around the globe, with new initiatives and programs announced almost daily, government adoption of blockchain remains relatively immature (as is true for other industries). The most advanced government use cases have achieved a pilot or proof-of-concept stage, but many are still exploratory. It is still not certain that blockchain will even take hold in governments; in some cases the technology appears to be a solution in search of a problem. A 2017 Gartner survey of 340 government CIOs/IT leaders indicated that just 7% think blockchain will be a big driver of change for their organization within the next five years.[136]

It is also not clear if blockchain will bring any cost savings to governments. A recent Accenture report concludes that, in the banking sector at least, savings from blockchain technologies will be dramatic – in the realm of 50% across all functions.[137] However, the report has been met with skepticism by some observers, who note that not only does it base its cost savings predictions on the ability of banks to replace legacy systems and infrastructure – an unlikely prospect – but it also fails to adequately account for exploding future costs in power and storage.[138]

5 BARRIERS AND CHALLENGES

As stated above, despite the attention distributed ledger technology has received in recent years, there are a number of challenges still to overcome if the expected benefits are to be realized. The most common criticisms and shortcomings can be summarized as follows:

- **The technology is not ready for prime time**. If everyone rushed to get bitcoin today, its blockchain would become unstable because its infrastructure lacks the transactional capacity to on-board millions of people. In other applications, interfaces are user-unfriendly, requiring a high tolerance for alphanumeric code, and users lack legal recourse because the law has yet to rule on the irrevocability of transactions and smart contracts.[139]
- **The energy consumed is unsustainable**. The proof-of-work method used to secure the bitcoin network uses an enormous and ever-increasing amount of electricity. [139]
- **Governments will stifle it**. Will the bitcoin blockchain network hold its own against entrenched central authorities? There must be a stable approach to regulation, legislation, and negotiation of treaties to minimize uncertainty, so that investors will continue to support development.
- **Powerful incumbents will usurp it**. Corporations captured and are now using the internet to extract most of its value. Will the same thing happen with blockchain? [139]
- **Governing the protocols is like herding cats**. Unlike the internet, the bitcoin community lacks formal oversight bodies to anticipate needs and guide their resolution. Community members prefer it that way but cannot agree on a way forward. If governance is not addressed, then the movement could collapse on itself as it disintegrates into warring factions. [139]
- **Big Brother is (still) watching you**. While blockchains ensure a degree of anonymity, they also provide a degree of openness. Corporations and countries known for spying will likely redouble their efforts because value is involved.[139]

Blockchain may also soon be reaching its peak (if it has not already), at least in terms of the hyperbole surrounding the technology in the past 18 months. In its 2018 *Hype Cycle for Emerging Technologies*[o], Gartner suggests blockchain has passed its "Peak of inflated expectations" and is sliding precipitously

[o] See https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/.

towards the "Trough of Disillusionment". However, Gartner also suggests that a specific application of the technology, *Blockchain for Data Security,* is near the beginning of the cycle.[140]

Regulatory constraints

Regulatory issues also represent a hurdle to widespread distributed ledger technology adoption. A recent survey found that two out of five business executives cited regulatory concerns as a barrier to further investment in blockchain.[141] DLT has started to infiltrate well-established areas where intermediaries have performed critical functions for decades, but the lack of regulation around new concepts and methods such as cryptographic signatures and smart contracts is helping to put the brakes on adoption. For example, some organizations are exploring the use of blockchain for securely sharing patient medical records, but existing privacy laws and regulations surrounding who can access (and who controls) personal records are fundamentally at odds with the blockchain model.[142]

So-called "regulatory sandboxes" might be one way to ease industry fears and guide blockchain technology into the mainstream. Such sandboxes are designed to help governments better understand a new technology and its regulatory implications, while at the same time giving industry an opportunity to test new technology and business models in a live environment. According to the OECD, current blockchain regulatory sandboxes mostly focus on financial technology, and are being developed in countries as diverse as Australia, Indonesia, Japan, Malaysia, Switzerland, Thailand and the United Kingdom, but the scope of sandboxes could be broadened to encompass blockchain applications in non-financial sectors.[11]

Governance is another concern. One of the principles of distributed ledger technology is that, by definition, ownership and control of the network (at least in permissionless systems) is distributed across the network rather than in the hands of a centralized authority like a government or corporation. However, many of the potential blockchain applications currently in development are also in highly important areas for the economy (for example payment systems) or the public good (government databases). These applications sometimes require direct government involvement given the nature of the information, meaning that policymakers will need make decisions about governance of the data; that is, to what degree private blockchain networks can provide services based on this kind of data and how governments engage with these networks. Prime examples are the Bank of Canada's Jasper project examining the feasibility of an interbank settlement engine, along with several foreign government projects to harmonize online identities.[120,143]

Legal and regulatory concerns around data privacy, intellectual property, enforceability of contracts, and choice of jurisdiction are inhibiting DLT adoption, but while regulation should not stifle innovation, it is nevertheless indispensable for creating a basic legal framework and putting standards into place that offer safety and stability.[143] It is also important to not leave governance to governments alone. Today the Internet is managed through standards networks like the Internet Engineering Task Force and World Wide Web Consortium. Policy groups like the Internet Governance Forum develop Internet policy and propose rules. Advocacy groups like the Electronic Frontier Foundation fight for an open Internet and protect the privacy of users. Operational networks such as Internet Committee for Assigned Names and Numbers deliver basic functions and infrastructure and dispense domain names.[144] If the potential of blockchain is to be fully realized, it may need a similar multi-stakeholder approach to regulation.

General Data Protection Regulation

In the European Union (EU), one of the major limitations for the mass adoption of blockchain is the General Data Protection Regulation (GDPR), which came into effect May 25, 2018. The GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[145] Data protection regulations ensure the rights of users to control access to personal data, including the right to be forgotten. Blockchain systems, in contrast, allow every participant to access the entire blockchain. In addition, blockchain transactions, and by extension the data stored in a blockchain, are immutable. In other words, once recorded, a transaction and the associated transaction data cannot be erased.[146]

However, while blockchain may appear to be at odds with data privacy requirements, that is not the case with permissioned applications. A public blockchain such as bitcoin may conflict with GDPR stipulations, but a blockchain does not need to be public. Further, although transaction data will be immutable, utilising blockchain applications does not dictate that personal data falling under GDPR protection must also be stored in an immutable blockchain.[147]

By using blockchain in the public sector, governments could also raise awareness of its potential when it improves on existing technologies. Technical issues will need to be resolved, such as how to trust the data placed on the blockchain; trustworthy data may need to be certified in some way. Blockchain may also raise concerns about competition policy, as some large corporations begin to mobilise through consortia to establish blockchain standards, e.g. for supply-chain management.

Military adoption

Many of these same challenges apply to blockchain use in the military, although one of the primary concerns is that, as a means of processing transactions, DLT is comparatively slow. Speed is a major requirement in a combat setting, where it can mean the difference between life and death. When many computers are involved, the transaction speeds of blockchain systems may be slower than alternative processes, at least with current technology. However, fast protocols operating on top of blockchain are under development,[11] and there has been some recent research into using quantum techniques to speed up the mining process and address scalability issues.[148] [149]

Blockchains are also not immune from attack, despite the high degree of security provided by cryptographically-linked blocks of data. They are susceptible to distributed denial-of-service (DDoS) incursions, which occur when multiple systems flood the bandwidth or resources of a system. Bitcoin and Ethereum have both been targets of DDoS attacks. Several papers have been published in the research literature proposing various methods to mitigate DDoS assaults on blockchains.[150-152]

The paper from Canada's Defence Research and Development Canada mentioned earlier, *On blockchain technology and its potential application in tactical networks*, notes several other challenges for blockchain in the military, in particular memory requirements; trust mechanisms; bandwidth constraints; network availability, consistency and size; blockchain length; and data verification and validation.[45] Interoperability between various blockchain platforms and solutions is another challenge for military applications—unless blockchain technology can be readily connected to existing systems, it will be of little utility.[153]

Better alternatives

Distributed ledger technology may be inspiring a new generation of financial services innovation and provide the foundation for cryptocurrencies like bitcoin, but it may not be the best solution for every problem. Distributed ledgers have been known and used for decades, but while previous distributed databases were permissioned and required a third party to manage the permissions and maintain the database, bitcoin was the first that allowed for a permissionless distributed ledger. So the uniqueness of bitcoin's blockchain is that it is virtually immutable without a need for a trusted third party. However, these benefits may be difficult to realize in a blockchain without bitcoin. It has proven to be a challenge to create a decentralized, permissionless and secure blockchain to transfer assets other than a native cryptocurrency.[16] There are two main reasons for this:

1. **The gateway problem**: The underlying assets need to enter the blockchain in the first place. Whether the gateway is an individual, an institution or a consortium, it needs to be a trusted third party for subsequent users of the blockchain. Bitcoin does not need a gateway since the currency is native to its blockchain.[16]

2. **Assuring immutability of the ledger without a native currency**. Bitcoin isn't secure because of blockchain; it is secure because the effort and cost of subverting its blockchain is greater than the value of what's being protected. The effort and cost that protect bitcoin comes in the form of time, computing power and electricity. The effort is dictated by the rules that are "baked in" to what bitcoin is. Without bitcoins (or other native cryptocurrency) as a reward, the network participants need to be motivated by incentives from outside of the blockchain.[16,154]

Both of the above challenges are typically addressed by creating a permissioned blockchain, or in other words, a traditional distributed database, in which case a blockchain may not be the most appropriate design choice for such a database in the first place. A chain is only as strong as its weakest link, which is equally true of blockchains; if one node has performance, scale or security problems, it can impact the others. Therefore, although a blockchain can be a powerful solution, organizations should consider using it only when they have challenges that are not better addressed by existing technology.[138]

6 CONCLUSION

The purpose of this study was to conduct a review of R&D activity in the domain of distributed ledger technology over the last ten years (2008-2018). In total, 2,520 bibliographic records from several scientific and technical databases were analyzed. Just over 51% of the documents were published in 2018 alone, two months before the year is complete—an indication of the recent and rapid rise of research interest in this topic. Much of the interest and excitement may be a by-product of the fact that blockchain (a type of DLT) is the underlying technology of bitcoin, the cryptocurrency experiencing spectacular growth and intense media attention over the last year.

DLT is attracting global research interest, with over 90 countries (led by the US and China) contributing to the scientific literature. The top publishing author-affiliations over the time frame are the Chinese Academy of Sciences (49 publications), IBM (48) and Australia's CSIRO (36). In Canada, the University of British Columbia is the most prolific entity, with 11 publications. The top military-related organizations in the dataset are China's National University of Defense Technology (19 publications), the US Air Force Research Laboratory (11) and the US Army Research Laboratory (5).

Findings from the literature analysis show that the potential application areas of DLT are diverse. The plethora of pilot projects underway indicate that both governments and private industry have embraced DLT as a potential solution to many problems. Military organizations around the world have also not been immune to the lure of DLT, with cyber defence, secure messaging, resilient communications and logistics support being the primary areas of focus. Going forward, DRDC may wish to monitor the numerous DLT initiatives and trials at the US Department of Defence and its various agencies and sub-departments, many of which have begun this year or will be underway soon.

However, despite the enthusiasm and excitement surrounding the potential of DLT, and blockchain in particular, the technology may not be able to live up to expectations. Today, most if not all initiatives are in the proof of concept or pilot phase, and even though a few have had positive results, none have run for long periods of time. Several barriers and challenges also deter widespread adoption, including regulatory concerns, energy requirements and questions as to whether a blockchain without a native currency is even viable, or can provide a better solution than existing technology. The benefits of encryption and smart contracts can be realized without a distributed ledger, and a blockchain alone is not what creates security, so organizations may need to ask themselves why running a blockchain is better than an ordinary database.

One of the unintended consequences of the intense interest in blockchain may be the popularization of traditional distributed databases, which have been around for decades. The current blockchain frenzy has brought distributed database technology into the limelight and may eventually result in wider adoption and new ideas for their use. Nevertheless, it is not clear that distributed databases in the form of blockchain will bring substantial cost savings over alternative technology. Ultimately, the blockchain revolution that many observers foresee may indeed provide new tools and indelibly impact many aspects of society but, in the words of one commentator, “the world after the blockchain revolution may well be a world without the blockchain.”[16]

Lastly, it is important to note that the aim of this study was not to conduct an expert technical evaluation of the systems, methods, processes and technologies identified, but to provide an overall picture of the current state of publicly-available R&D activity in the area of DLT. The trends identified in this report are derived from statistical analyses of keywords and subject headings and not on a thorough and careful reading of all the available literature. For more insightful conclusions and to capture important details that may be overlooked by a broad survey, a systematic and in-depth review of the literature dataset (provided as an accompaniment to this report) by a subject specialist is recommended.

7 REFERENCES

1. Sudhan A, Nene MJ. Employability of blockchain technology in defence applications. *2017 International Conference on Intelligent Sustainable Systems (ICISS). Proceedings.* 2017:630-637. http://dx.doi.org/10.1109/ISS1.2017.8389247.
2. Tapscott D, Tapscott A. How Canada can be a global leader in blockchain technology. *The Globe and Mail.* May 17, 2018. https://www.theglobeandmail.com/report-on-business/rob-commentary/how-canada-can-be-a-global-leader-in-blockchain-technology/article34259697/.
3. Chew B, Henry W, Lora A, Chae H. *Assessing blockchain applications for the public sector*. *Deloitte Insights.* September 7, 2018. https://www2.deloitte.com/insights/us/en/industry/public-sector/blockchain-public-sector-applications.html.
4. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System* 2008, https://bitcoin.org/bitcoin.pdf
5. Doubleday K. *Blockchain for 2018 and Beyond: A (growing) list of blockchain use cases*. *Medium.com.* 2018. https://medium.com/fluree/blockchain-for-2018-and-beyond-a-growing-list-of-blockchain-use-cases-37db7c19fb99.
6. Acuña O. *Deloitte outlines obstacles to mainstream adoption of blockchain*. *Coin Rivet.* October 2, 2018. https://www.coinrivet.com/deloitte-outlines-obstacles-to-mainstream-adoption-of-blockchain/.
7. Williams M. *Counterfeit parts are costing the industry billions*. *Automotive Logistics.* 2013. https://automotivelogistics.media/intelligence/16979.
8. Mearian L. *Blockchain integration turns ERP into a collaboration platform*. *Computerworld.* 2017. https://www.computerworld.com/article/3199977/enterprise-applications/blockchain-integration-turns-erp-into-a-collaboration-platform.html.
9. Weston G. *Fake parts in Hercules aircraft called a genuine risk*. 2013. https://www.cbc.ca/news/politics/fake-parts-in-hercules-aircraft-called-a-genuine-risk-1.1345862.
10. European Commission. *#Blockchain4EU: Blockchain for Industrial Transformations.* Luxembourg: Publications Office of the European Union 2018, https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain4eu-blockchain-industrial-transformations
11. Guellec D, Keenan M, Larrue P, Fraccola S. *Impacts and Policies Surrounding the Technologies of the Next Production Revolution.* : OECD October 16, 2018,
12. Port of Montreal. *The Port of Montreal joins Maersk/IBM TradeLens platform*. 2018. https://www.port-montreal.com/en/tradelens-en.html.
13. *FaceMe To Accelerate AI Innovation Using Tatau's Distributed Supercomputer*. *Digital Journal.* October 31, 2018. http://www.digitaljournal.com/pr/4006521#ixzz5VdcInJuk.
14. Wang B. *Does the ever-growing artificial intelligence sector need the services of blockchain technology? Next Big Future.* November 1, 2018. https://www.nextbigfuture.com/2018/11/does-the-ever-growing-artificial-intelligence-sector-need-the-services-of-blockchain-technology.html.
15. Gartner. *Blockchain-Based Transformation: A Gartner Trend Insight Report.* March 2018, https://www.gartner.com/doc/3869696/blockchainbased-transformation-gartner-trend-insight
16. Halaburda H. Blockchain revolution without the blockchain? *Commun. ACM.* 2018;61(7):27-29. http://dx.doi.org/10.1145/3225619.
17. UK Government Office for Science. *Distributed Ledger Technology: beyond block chain*. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

18. Kaminska I. *Growing scepticism challenges the blockchain hype*. *Financial Times.* June 20, 2017. https://www.ft.com/content/b5b1a5f2-5030-11e7-bfb8-997009366969.
19. LeewayHertz. Blockchain Platforms used by Top Blockchain Companies 2018: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/.
20. Liang X, Zhao J, Shetty S, Li D. Towards data assurance and resilience in IoT using blockchain. 2017. http://dx.doi.org/10.1109/MILCOM.2017.8170858.
21. Li R, Song T, Mei B, Li H, Cheng X, Sun L. Blockchain For Large-Scale Internet of Things Data Storage and Protection. *IEEE Trans. Serv. Comput.* 2018. http://dx.doi.org/10.1109/TSC.2018.2853167.
22. Wang J, Li M, He Y, Li H, Xiao K, Wang C. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. *IEEE Access.* 2018;6:17545-17556. http://dx.doi.org/10.1109/ACCESS.2018.2805837.
23. University of British Columbia. Blockchain@UBC 2018: https://blockchainubc.ca.
24. Daniel J, Sargolzaei A, Abdelghani M, Sargolzaei S, Amaba B. Blockchain Technology, Cognitive Computing, and Healthcare Innovations. *Journal of Advances in Information Technology.* 2017;8(3):194-198. http://dx.doi.org/10.12720/jait.8.3.194-198.
25. Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B. *Blockchain technology innovations*. *2017 IEEE Technology & Engineering Management Conference (TEMSCON).* 2017:137-141.
26. Vo HT, Mehedy L, Mohania M, Abebe E. Blockchain-based data management and analytics for micro-insurance applications. 2017. http://dx.doi.org/10.1145/3132847.3133172.
27. Nath I. Data Exchange Platform to Fight Insurance Fraud on Blockchain. *2016 IEEE 16th International Conference on Data Mining: Workshops (ICDMW).* 2016:821-825. http://dx.doi.org/10.1109/ICDMW.2016.0121.
28. Samaniego M, Deters R. Blockchain as a Service for IoT. 2017. http://dx.doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.
29. Samaniego M, Deters R. Hosting virtual IoT resources on edge-hosts with blockchain. 2017. http://dx.doi.org/10.1109/CIT.2016.71.
30. Campbell-Verduyn M. Introduction: What are blockchains and how are they relevant to governance in the global political economy? *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Glob. Gov.* 2017:1-24. http://dx.doi.org/10.4324/9781315211909.
31. Campbell-Verduyn M. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime Law Soc. Change.* 2018;69(2):283-305. http://dx.doi.org/10.1007/s10611-017-9756-5.
32. Liu Y, Liu X, Zhang L, Tang C, Kang H. An efficient strategy to eliminate malleability of bitcoin transaction. 2018. http://dx.doi.org/10.1109/ICSAI.2017.8248424.
33. Yuan Y, Wang FY. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems.* 2018;48(9):1421-1428. http://dx.doi.org/10.1109/TSMC.2018.2854904.
34. Liu Y, Liu X, Tang C, Wang J, Zhang L. Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin. *IEEE Access.* 2018;6:23261-23270. http://dx.doi.org/10.1109/ACCESS.2018.2827163.
35. Liu Y, Chen X, Zhang L, Tang C, Kang H. An intelligent strategy to gain profit for bitcoin mining pools. In: proceedings from Proceedings - 2017 10th International Symposium on Computational Intelligence and Design, ISCID 20172018. http://dx.doi.org/10.1109/ISCID.2017.184.
36. Zheng Z, Xie S, Dai H, Chen X, Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017. http://dx.doi.org/10.1109/BigDataCongress.2017.85.
37. Fangyu G, Baosheng W, Wenping D, Wei P. Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network. *Database Systems for Advanced Applications. 23rd*

International Conference, DASFAA 2018. Proceedings: LNCS 10828. 2018:666-681. http://dx.doi.org/10.1007/978-3-319-91458-9_41.

38. Nikouei SY, Ronghua X, Nagothu D, Yu C, Aved A, Blasch E. Real-Time Index Authentication for Event-Oriented Surveillance Video Query using Blockchain. *arXiv.* 2018:8. http://arxiv.org/abs/1807.06179.
39. Qiwu Z, Yuzhe T, Ju C, et al. ChainFS: blockchain-secured cloud storage. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD).*987-990. http://dx.doi.org/10.1109/CLOUD.2018.00152.
40. Tosh D, Shetty S, Foytik P, Kamhoua C, Njilla L. CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD).*302-309. http://dx.doi.org/10.1109/CLOUD.2018.00045.
41. Tosh DK, Shetty S, Liang X, Kamhoua CA, Kwiat KA, Njilla L. Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack. 2017. http://dx.doi.org/10.1109/CCGRID.2017.111.
42. Saad M, Mohaisen A, Kamhoua C, Kwait K, Njilla L. Countering Double-Spending in Next-Generation Blockchains. 2018. http://dx.doi.org/10.1109/ICC.2018.8423019.
43. Tosh DK, Shetty S, Liang X, Kamhoua C, Njilla L. Consensus protocols for blockchain-based data provenance: Challenges and opportunities. 2018. http://dx.doi.org/10.1109/UEMCON.2017.8249088.
44. Rawat DB, Njilla L, Kwiat K, Kamhoua C. IShare: Blockchain-Based Privacy-Aware Multi-Agent Information Sharing Games for Cybersecurity. 2018. http://dx.doi.org/10.1109/ICCNC.2018.8390264.
45. Willink TJ. *On Blockchain Technology and its Potential Application in Tactical Networks.* Ottawa, ON, Canada: Defence Research and Development Canada; 01 Apr 2018 2018. DRDC-RDDC-2018-R033, http://pubs.drdc-rddc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3DSYSNUM=806401&r=0
46. Garcia P. Biometrics on the blockchain. *Biometric Technology Today.* 2018;2018(5):5-7. http://dx.doi.org/10.1016/S0969-4765(18)30067-5.
47. Dunphy P, Petitcolas FAP. A First Look at Identity Management Schemes on the Blockchain. *IEEE Security & Privacy.* 2018;16(4):20-29. http://dx.doi.org/10.1109/MSP.2018.3111247.
48. Wolfond G. A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review.* October 2017;7(10):35-40.
49. Azouvi S, Al-Bassam M, Meiklejohn S. *Who Am I? Secure Identity Registration on Distributed Ledgers*. 2017:373-389.
50. Barnas NB. *Blockchains in national defense: trustworthy systems in a trustless world* Maxwell Air Force Base 2016, http://www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/barnas_n.pdf
51. Semiconductor Industry Association. *Winning the Battle Against Counterfeit Semiconductor Products: A Report of the SIA Anti-Counterfeiting Task Force.* 2013, https://www.semiconductors.org/clientuploads/Anti-Counterfeiting/SIA%20Anti-Counterfeiting%20Whitepaper.pdf
52. Ravich S. *Leveraging Blockchain Technology to Protect the National Security Industrial Base*: Foundation for Defense of Democracies July 10, 2017, https://www.fdd.org/analysis/2017/07/10/leveraging-blockchain-technology-to-protect-the-national-security-industrial-base/

53. Rothrie S. *Blockchain military applications: The future tech of the armed forces*. *Coin Central.* 2018 (June 25). https://coincentral.com/blockchain-military-applications-the-future-tech-of-the-armed-forces/.
54. Babones S. *Smart 'Blockchain Battleships' Are Right Around the Corner*. *Thae National Interest.* May 17, 2018. https://nationalinterest.org/feature/smart-battleships-are-right-around-the-corner-25872.
55. Dizikes P. *Study: On Twitter, false news travels faster than true stories MIT News.* March, 2018. http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.
56. Huckle S, White M. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains. *Big Data.* Dec 2017;5(4):356-371. http://dx.doi.org/10.1089/big.2017.0071.
57. Korta SM. *Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security*: Naval Postgraduate School 2018, https://www.hsdl.org/?abstract&did=811312
58. Patel D, Balakarthikeyan, Mistry V. Border Control and Immigration on Blockchain. *Blockchain - ICBC 2018. First International Conference Held as Part of the Services Conference Federation, SCF 2018. Proceedings: LNCS 10974.* 2018:166-179. http://dx.doi.org/10.1007/978-3-319-94478-4_12.
59. KPMG. *The National Defense Authorization Act for Fiscal Year 2018 - Perspectives on Cyberscecurity Policies and Implementation.* 2018, https://institutes.kpmg.us/government/articles/2018/national-defense-authorization-act-for-fiscal-year-2018.html
60. Gault M. *Blockchain and Implications for Trust in Cybersecurity*. March 16, 2018. https://guardtime.com/blog/blockchain-and-implications-for-trust-in-cybersecurity.
61. Galois. Galois and Guardtime Federal Awarded $1.8M DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System. 2016. https://galois.com/news/galois-guardtime-formal-verification/.
62. Wong JI. *Even the US military is looking at blockchain technology—to secure nuclear weapons*. Oct. 2016. https://qz.com/801640/darpa-blockchain-a-blockchain-from-guardtime-is-being-verified-by-galois-under-a-government-contract/.
63. Hamilton D. *DARPA Blockchain Programs*. *Coin Central.* Oct. 2016. https://coincentral.com/darpa-blockchain-programs/.
64. U.S. General Services Administration's Emerging Citizen Technology Office. Blockchain Programs 2018: https://emerging.digital.gov/blockchain-programs/.
65. Defense USDo. Department of Defense Fiscal Year (FY) 2019 Budget Estimates. February, 2018. https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/budget_justification/pdfs/03_RDT_and_E/RDTE_DAs_Vol_3A_of_5_OSD_FY19PB-RDTE_Exhibits_BA1-3.pdf.
66. Department of Defense. Sharing of Defense Research, Development, Testing, and Evaluation (RDT&E) Data Distribution using Distributed Ledger Technologies 2018: https://www.sbir.gov/sbirsearch/detail/1508913.
67. U.S. Navy. Clearinghouse for Subsistence Ordering & Receipt (CSOR) 2018: https://www.sbir.gov/sbirsearch/detail/1482697.
68. Staff writers. *U.S. Navy Looks to Blockchain Revolution*. *The Maritime Executive.* 2017. https://maritime-executive.com/article/us-navy-looks-to-blockchain-revolution.
69. U.S. Navy. DON Innovator Embraces a New Disruptive Technology: Blockchain 2018: http://www.secnav.navy.mil/innovation/Pages/2017/06/BlockChain.aspx.
70. U.S. Navy. Navy Approved Multi-Factor Authentication for Personal Mobile Devices 2018: https://www.sbir.gov/sbirsearch/detail/1473595.

71. ITAMCO. Naval Aviation Enterprise Exploring Blockchain With Indiana-Based Company ITAMCO2018. https://www.prnewswire.com/news-releases/naval-aviation-enterprise-exploring-blockchain-with-indiana-based-company-itamco-300716633.html.
72. U.S. Department of Defense Special Operations Command. Automated Processing, Exploitation and Dissemination 2018: https://www.sbir.gov/sbirsearch/detail/1413791.
73. U.S. Department of Defense Defense Microelectronics Activity. Blockchain Supply Chain Enhancement for Trusted & Assured FPGAs and ASICs 2018: https://www.sbir.gov/sbirsearch/detail/1482583.
74. U.S. Department of Homeland Security. Blockchain Applications for Homeland Security Missions. 2017. https://www.sbir.gov/sbirsearch/detail/1227405.
75. U.S. Department of Homeland Security. Decentralized Key Management using Blockchain. 2017. https://www.sbir.gov/sbirsearch/detail/1302463.
76. Manning J. *Factom Receives Another DHS Grant For Blockchain IoT Project*. *ETH News.* June, 2018. https://www.ethnews.com/factom-receives-second-dhs-grant-for-blockchain-iot-project.
77. U.S. Department of Homeland Security. S&T Leading Blockchain Solution R&D for DHS Components 2018: https://www.dhs.gov/science-and-technology/blog/2018/05/22/st-leading-blockchain-solution-rd-dhs-components.
78. National Science Foundation. Distributed Ledger. September, 2018: https://www.sbir.gov/sbirsearch/detail/1519895.
79. Crossword Cybersecurity. Crossword wins contract with MOD's Defence Science and Technology Laboratory to create blockchain enabled smart documents 2016: https://www.crosswordcybersecurity.com/2016/05/25/2016-5-crossword-wins-contract-with-mods-defence-science-and-technology-laboratory-to-create-blockchain-enabled-smart-documents/.
80. Reuters. *For security agencies, blockchain goes from suspect to potential solution*. *ETCIO.com.* December, 2017. https://cio.economictimes.indiatimes.com/news/digital-security/for-security-agencies-blockchain-goes-from-suspect-to-potential-solution/61910963.
81. Cowan G. *Companies Look to Blockchain To Secure Supply Chains*. *AIN Online.* July 2018. https://www.ainonline.com/aviation-news/aerospace/2018-07-12/companies-look-blockchain-secure-supply-chains.
82. Shen M. *The Russian Military Is Building a Blockchain Research Lab*. *Coindesk.* July 2, 2018. https://www.coindesk.com/the-russian-military-is-building-a-blockchain-research-lab/.
83. Rhodes D. *Improving Defense Industry Technology with Blockchain*. *Coin Central.* June 15, 2018. https://coincentral.com/defense-industry-technology/.
84. Staff writers. *Blockchain technology may be introduced in Russia's armed forces*. *Tass.* 2017. http://tass.com/defense/961423.
85. Sanchez SL. *Blockchain Technology in Defence*. *European Defence Matters.* 2017(14). https://www.eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence.
86. Jones S. *How new database innovations multiply blockchain use*. *Smart Data Collective.* 2018 (October 10). https://www.smartdatacollective.com/how-new-database-innovations-multiply-blockchain-use/
87. Burhanuddin NS, Zaman FHK, Yassin AIM, Tahir NM. Blockchain in voting system application. *Int. J. Eng. Technol.* 2018;7(4):156-162. http://dx.doi.org/10.14419/ijet.v7i4.11.20793.
88. Khan KM, Arshad J, Khan MM. Secure Digital Voting System Based on Blockchain Technology. *International Journal of Electronic Government Research.* 2018;14(1):53-62. http://dx.doi.org/10.4018/IJEGR.2018010103.

89. Mudliar K, Parekh H. A comprehensive integration of national identity with blockchain technology. In: proceedings from 3rd International Conference on Communication, Information and Computing Technology, ICCICT 20182018. http://dx.doi.org/10.1109/ICCICT.2018.8325891.
90. Sullivan C, Burger E. E-residency and blockchain. *Computer Law and Security Review*. 2017;33(4):470-481. http://dx.doi.org/10.1016/j.clsr.2017.03.016.
91. Conference Board of Canada. *Cautious Optimism: Adopting Blockchain to Improve Canadian Government Digital Services*. Ottawa: Conference Board of Canada; 2018.
92. Government of the Netherlands. *Blockchain Projects.* 2018: https://www.blockchainpilots.nl/home-eng.
93. Johnson P. Partnering for a path to digital identity. *Microsoft Official Blog*2018. https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/.
94. Cheng S, Daub M, Domeyer A, Lundqvist M. *Using blockchain to improve data management in the public sector*. *Digital McKinsey.* 2017 (February). https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector.
95. Desouza KC, Ye C, Somvanshi KK. *Blockchain and U.S. state governments: An initial assessment*. *Brookings Institution.* 2018 (April 17). https://www.brookings.edu/blog/techtank/2018/04/17/blockchain-and-u-s-state-governments-an-initial-assessment/.
96. U.S. Government Services Administration. *Blockchain.* 2018: https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain.
97. Mackey TK, Nayyar G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opin. Drug Saf.* 2017;16(5):587-602. http://dx.doi.org/10.1080/14740338.2017.1313227.
98. Sylim P, Liu F, Marcelo A, Fontelo P. Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *J. Med. Internet Res.* 2018;20(9). http://dx.doi.org/10.2196/10163.
99. Galvez JF, Mejuto JC, Simal-Gandara J. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends Anal. Chem.* 2018;107:222-232. http://dx.doi.org/10.1016/j.trac.2018.08.011.
100. Orcutt M. *The the CDC wants in on blockchain*. *MIT Technology Review.* 2017 (October 2). https://www.technologyreview.com/s/608959/why-the-cdc-wants-in-on-blockchain/.
101. Melendez S. *How IBM and the CDC are testing blockchain to track health issues like the opioid crisis*. *Fast Company.* 2018 (September 4). https://www.fastcompany.com/90231255/how-ibm-and-the-cdc-are-testing-blockchain-to-track-health-issues-like-the-opioid-crisis.
102. Biswas K, Muthukkumarasamy V. Securing Smart Cities Using Blockchain Technology. In: proceedings from 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS); 12-14 Dec. 2016, 2016. http://dx.doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198.
103. Magas J. *Smart cities and blockchain: Four countries where AI and DLT exist hand-in-hand*. *Cointelegraph.* 2018 (June 18). https://cointelegraph.com/news/smart-cities-and-blockchain-four-countries-where-ai-and-dlt-exist-hand-in-hand.
104. PwC. *Blockchain: The Next Innovation to Make our Cities Smarter*: PwC India; 2018: https://www.pwc.in/assets/pdfs/publications/2018/blockchain-the-next-innovation-to-make-our-cities-smarter.pdf.

105. Basden J, Cottrell M. *How utilities are using blockchain to modernize the grid*. *Harv. Bus. Rev.* 2017 (March). https://hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid.
106. Delahunty S. *Developments and adoption of blockchain in the U.S. federal government*. *Forbes.* 2018(January 28). https://www.forbes.com/sites/forbestechcouncil/2018/01/25/developments-and-adoption-of-blockchain-in-the-u-s-federal-government/#2001c60b3d99.
107. Verrico J. *DHS S&T Awards $199K to Austin Based Factom Inc. for Internet of Things Systems Security.* Washington, DC: Department of Homeland Security; 2016 https://www.dhs.gov/science-and-technology/news/2016/06/17/st-awards-199k-austin-based-factom-inc-iot-systems-security.
108. Banerjee M, Lee J, Choo KKR. A blockchain future for internet of things security: a position paper. *Digit. Commun Netw.* 2018;4(3):149-160. http://dx.doi.org/10.1016/j.dcan.2017.10.006.
109. Adkins C, Ellis D. *Protecting the Additive Manufacturing Workflow with Blockchain Technology*. Ann Arbor, MI: National Center for Manufacturing Services; 2018.
110. Ivanov D, Dolgui A, Sokolov B. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *Int J Prod Res.* 2018:1-18. http://dx.doi.org/10.1080/00207543.2018.1488086.
111. Gottlieb C. *Blockchain in Aerospace and Defense*: Accenture; 2017: https://www.accenture.com/t20170928T023222Z__w__/us-en/_acnmedia/PDF-61/Accenture-Blockchain-For-Aerospace-Defense-PoV-v2.pdf.
112. Friedman S. *FDA builds blockchain-based health data sharing platform*. *GCN.* 2018 (June 22). https://gcn.com/articles/2018/06/22/fda-blockchain-ehr-sharing.aspx.
113. Mearian L. *IBM Watson, FDA to explore blockchain for secure patient data exchange*. *Computerworld.* 2017 (January 11). https://www.computerworld.com/article/3156504/healthcare-it/ibm-watson-fda-to-explore-blockchain-for-secure-patient-data-exchange.html.
114. Linver H. *Government Bonds: How Blockchain Can Beat the Red Tape. Coin Telegraph.* October 3, 2018. https://cointelegraph.com/news/government-bonds-how-blockchain-can-beat-the-red-tape.
115. Berryhill J, Bourgery T, Hanson A. *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector.* Paris: OECD;2018, http://dx.doi.org/10.1787/3c32c429-en
116. Althauser J. *US General Services Agency Launches Information Portal Listing Possible Blockchain Technology Applications.* . Aug. 10, 2017. https://cointelegraph.com/news/us-general-services-agency-launches-information-portal-listing-possible-blockchain-technology-applications.
117. Institute on Governance. *Blockchain in Government Workshop - Summary Report.* 2018, https://iog.ca/docs/Blockchain-in-Government-Workshop-Summary-Report.pdf
118. National Research Council Canada. NRC-IRAP - Blockchain publishing prototype 2018: https://nrc-cnrc.explorecatena.com/en/.
119. National Research Council Canada. Exploring blockchain for better business. August, 2018: https://www.nrc-cnrc.gc.ca/eng/stories/2018/blockchains.html.
120. Bank of Canada. FINTECH experiments and projects. 2018: https://www.bankofcanada.ca/research/digital-currencies-and-fintech/fintech-experiments-and-projects/.
121. Digital ID & Authentication Council of Canada. Is Blockchain the Answer to Corporate Registries in Canada? 2017: https://diacc.ca/2017/06/06/is-blockchain-the-answer-to-corporate-registries-in-canada/.

122. Macaulay T. *How governments around the world are using blockchain. . ComputerWorld UK.* October 2, 2018. https://www.computerworlduk.com/galleries/applications/how-governments-are-using-blockchain-3680393/.
123. Oleinic A. *Estonia is Beating China and the US in Blockchain Adoption*. September 18, 2018. https://blocklr.com/news/estonia-beating-china-us-blockchain-adoption/.
124. Whitehouse D. *Should we put our trust in blockchain? . Global Government Forum.* November 6, 2018. https://www.globalgovernmentforum.com/should-we-put-our-trust-in-blockchain/.
125. Clarke L. *How is the UK government using blockchain? ComputerWorld UK.* October 2, 2018. https://www.computerworlduk.com/infrastructure/how-is-uk-government-using-blockchain-3684629/.
126. Anderson R. *Dubai to use blockchain technology for all government documents by 2020*. *Gulf Business.* 2016. http://gulfbusiness.com/dubai-use-bitcoin-database-technology-government-documents-2020/.
127. Nordrum A. Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything. *IEEE Spectrum.* 2017;54(10):54-55. http://dx.doi.org/10.1109/MSPEC.2017.8048841.
128. Blows N. *Dubai plans to launch 20 blockchain-based services in 2018.* January 16, 2018. https://bitcoinist.com/dubai-plans-launch-20-blockchain-based-services-2018/.
129. Hou H. The application of blockchain technology in E-government in China. 2017. http://dx.doi.org/10.1109/ICCCN.2017.8038519.
130. Southurst J. *Chinese Government Publishes Blockchain Financial Whitepaper*. *Bitcoin.com.* 2016. https://news.bitcoin.com/chinese-government-blockchain-whitepaper/.
131. Zhao W. *PBoC-Backed Blockchain Trade Finance Platform Enters Test Phase*. September 4, 2018. https://www.coindesk.com/pboc-backed-blockchain-trade-finance-platform-enters-test-phase.
132. Ngetich D. *Forget Bitcoin, this is How China Plans to Dominate the $102 Trillion Blockchain Space*. *Ethereum World News.* October 3, 2018. https://ethereumworldnews.com/china-dominate-blockchain/.
133. O'Brien K. *In China the mantra remains" blockchain not bitcoin"*. *Bitcoinist.* September 18, 2018. https://bitcoinist.com/chinas-long-march-to-dominance-behind-the-blockchain-not-bitcoin-mantra/.
134. Hackett R. *Walmart and IBM Are Partnering to Put Chinese Pork on a Blockchain. . Fortune.* 2016. http://fortune.com/2016/10/19/walmart-ibm-blockchain-china-pork/.
135. Liao S. *China will soon require blockchain users to register with their government IDs*. *The Verge.* October 22, 2018. https://www.theverge.com/2018/10/22/18008640/china-blockchain-registration-government-id.
136. Holgate R, Furlonger D, Howard R. *Toolkit: Government Use Cases for Blockchain.*: Gartner 2017, https://www.gartner.com/doc/3615119/toolkit-government-use-cases-blockchain
137. Accenture. *Banking on blockchain.* 2017, https://www.accenture.com/us-en/insight-banking-on-blockchain
138. Bloomberg J. *Don't Let Blockchain Cost Savings Hype Fool You*. *Forbes.* February 24, 2018. https://www.forbes.com/sites/jasonbloomberg/2018/02/24/dont-let-blockchain-cost-savings-hype-fool-you/.
139. Tapscott A, Tapscott D. *The Blockchain Corridor: Building an Innovation Economy in the 2nd Era of the Internet.* 2017, https://www.blockchaindailynews.com/attachment/813330/
140. *Gartner Hype Cycle for Emerging Technologies.* 2018, https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

141. Deloitte. *2018 global blockchain survey*, https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html
142. Miliard M. *Blockchain and healthcare privacy laws just don't mix*. *Healthcare IT News.* 2017. https://www.healthcareitnews.com/news/blockchain-and-healthcare-privacy-laws-just-dont-mix.
143. Koeppl T, Kronick J. *Blockchain Technology – What's in Store for Canada's Economy and Financial Markets?*: C.D. Howe Institute; 2017: https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Commentary_468_0.pdf.
144. Tapscott D. *2018 Blockchain Regulation Roundtable - Addressing the Regulatory Challenges of Disruptive Innovation*: Blockchain Research Institute August, 2018, https://s3.us-east-2.amazonaws.com/briwebinars/Tapscott_2018+Blockchain+Regulation+Roundtable_Blockchain+Research+Institute.pdf
145. Wikipedia contributors. General Data Protection Regulation 2018: https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&oldid=867704085.
146. Zhydik O. Has anyone done cost benefit analysis of any Blockchain use case? 2018: https://www.quora.com/Has-anyone-done-cost-benefit-analysis-of-any-Blockchain-use-case.
147. GDPR Compliance and Blockchain: Friends or Foes? 2018: https://eleks.com/blog/gdpr-compliance-and-blockchain-friends-foes/.
148. Ablayev FM, Bulychkov DA, Sapaev DA, Vasiliev AV, Ziatdinov MT. Quantum-Assisted Blockchain. *Lobachevskii J. Math.* 2018;39(7):957-960. http://dx.doi.org/10.1134/S1995080218070028.
149. Kiktenko EO, Pozhar NO, Anufriev MN, et al. Quantum-secured blockchain. *Quantum Science and Technology.* 2018;3(3). http://dx.doi.org/10.1088/2058-9565/aabc6b
150. Kim K, You Y, Park M, Lee K. DDoS Mitigation: Decentralized CDN Using Private Blockchain2018. http://dx.doi.org/10.1109/ICUFN.2018.8436643.
151. Rodrigues B, Bocek T, Stiller B. Multi-domain DDoS Mitigation Based on Blockchains. Security of Networks and Services in an All-Connected World. 11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management and Security, AIMS 2017. Proceedings: LNCS 10356.; 2017; Switzerland.
152. Rodrigues B, Bocek T, Lareida A, Hausheer D, Rafati S, Stiller B. A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. *Security of Networks and Services in an All-Connected World. 11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management and Security, AIMS 2017. Proceedings: LNCS 10356.* 2017:16-29. http://dx.doi.org/10.1007/978-3-319-60774-0_2.
153. Deloitte Insights. Blockchain and the five vectors of progress September 28, 2018: https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/value-of-blockchain-applications-interoperability.html.
154. Hampton N. *Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin. . Computerworld.* 2016. https://www.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/.

8 APPENDICES

8.1 Attachments

The following files are provided as separate attachments to this report.

- **Scientometric Study on Distributed Ledger Technology – Literature References.xlsx.** Contains the complete bibliographic references for the analyzed publications, including assigned subject groups. Links to the full-text are provided where available (note that due to licensing restrictions imposed by the database vendors, abstracts are not included).
- **Scientometric Study on Distributed Ledger Technology – Tableau Files.twbx** (requires download of the Tableau Reader at http://www.tableau.com/products/reader). Contains raw data files for the co-occurrence matrices and research momentum graphs (Figures 10-15).

8.2 Methodology

8.2.1 Search Strategy

Literature searches were conducted in the databases listed below.

- Scopus
- Inspec
- NTIS (US National Technical Information Service)
- DTIC (the US Defence Technical Information Centre)
- NATO Scientific and Technology Organization (STO)
- Canada.gc.ca (Canadian federal government web portal)
- Science.gov (US government science portal)
- Funding databases: Natural Sciences and Engineering Research Council of Canada (NSERC) and U.S. Small Business Innovation Research (SBIR)

In addition, several Internet searches were performed to capture other documents not typically published through normal distribution channels or indexed in commercial databases.

8.2.2 Analysis

Literature references were imported into VantagePoint software for cleaning and analysis. VantagePoint facilitates the creation of various groupings, statistical analyses, matrices, graphs, and cross-correlations to analyze the data and profile the activities of the major players. Other analytical tools such as Tableau and TouchGraph Navigator were used to generate graphs based on statistical operations performed in VantagePoint.

8.2.3 R&D Momentum

The R&D Momentum indicator is designed to identify rapidly rising subjects with relatively few publications. The challenge of identifying such subjects lies with the publication volume as a confounding factor, as their rapid growth and evolution is dwarfed by the high volume of established subjects. Specifically, the notion of "emerging" consists not only of a sharply rising trend line but also of

a small footprint in the domain of interest. A relatively small footprint is the reason emerging subjects are often overlooked until their disruptive impacts become obvious. In the Momentum indicator, the two parameters correspond to (1) growth rate which is the slope of a subject's trend line (right-left axis), and (2) volume which is the cumulated total number of publications (vertical axis).

Once growth rate and volume are separated, a two-dimensional coordinate can be used to plot a group of subjects. To do so, the two parameters have to be normalized with z-scores. The normalization process converts two sets of values in different units into the same measure by means of standard deviation, which also standardizes the variations for each of the two parameters. The four-quadrant visualization provides a structured view of the relative position of these subjects within the group.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.) NRC-Intelligence and Analytics 1200 Montreal Rd., Ottawa, ON K1A 0R6	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) **UNCLASSIFIED**

3. TITLE

Scientometric Study on Distributed Ledger Technology (Blockchain)

4. AUTHORS

Mike Culhane

5. DATE OF PUBLICATION	6a. NO. OF PAGES	6b. NO. OF REFS (Total cited in document.)
November 30, 2018	52 p.	154

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada
Ottawa, Ontario
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT PUBLIC RELEASE (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT PUBLIC RELEASE (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Public Release (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement
audience may be selected.))

Unlimited

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

National Research Council (NRC)
1200 Montreal Road, Building M-58
Ottawa, Ontario
K1A 0R6 Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Scientometric Study on Distributed Ledger Technology (Blockchain)

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Culhane, M.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
November 2018	53	154

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Valcartier Research Centre
Defence Research and Development Canada
2459 route de la Bravoure
Québec (Québec) G3J 1X5
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
NRC-NSL Project Number: MC19-005	FE22071907

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2019-C059	

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public Release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

distributed ledger technology; blockchain

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Abstract

DRDC commissioned this scientometric study on distributed ledger technology (DLT) with a view to understanding the potential impact of new research on future security and defence capabilities and operations. To answer the questions posed in the mandate, publication references from the past 10 years were retrieved and analyzed using text mining software and a variety of information visualization tools.

In total, 2,520 journal articles, conference papers, theses, books and government reports were published on DLT in the scientific literature between January 1, 2008 and October 1, 2018, and the number is growing rapidly. Just over 51% have been published so far in 2018 alone, a testament to the velocity of research interest recently. An analysis of an aggregated field of keyword subject groups created from the set of 2520 documents shows that some of the primary topics of R&D interest are cryptocurrencies, data security, applications and the Internet of Things. The top publishing author-affiliations are the Chinese Academy of Sciences (49 publications), IBM (48) and Australia's CSIRO (36). In Canada, the University of British Columbia is the most prolific entity, with 11 publications. The top military-related organizations in the dataset are China's National University of Defense Technology (19 publications), the US Air Force Research Laboratory (11) and the US Army Research Laboratory (5).

According to the literature, potential applications of distributed ledger technology, in particular blockchain, appear to be almost limitless and are projected to radically impact many industries in the coming years. For governments, DLT could help to streamline healthcare delivery, improve the collection of taxes, issue more secure passports and generally ensure the integrity of government records and services. For defense and security organizations, the technology promises to make supply chains more secure and efficient, protect sensitive data and communications, and enable more effective identity management.

However, despite the recent enthusiasm and surge of DLT initiatives around the world, whether the technology will live up to the lofty expectations is still up for debate. Several barriers and challenges remain, such as regulatory concerns, energy requirements and whether a blockchain without a native currency is even viable, or can provide a better solution than existing technology

Résumé

RDDC a commandé cette étude scientométrique sur la technologie de registres distribués (TRD) afin de comprendre l'impact potentiel des nouvelles recherches sur les capacités et les opérations de sécurité et de défense futures. Pour répondre aux questions posées dans le mandat, les références de publication des 10 dernières années ont été extraites et analysées à l'aide d'un logiciel d'extraction de texte et de divers outils de visualisation d'informations.

Au total, 2 520 articles de revues, conférences, thèses, ouvrages et rapports gouvernementaux ont été publiés sur la TRD dans la littérature scientifique entre le 1er janvier 2008 et le 1er octobre 2018, et leur nombre augmente rapidement. Un peu plus de 51% ont été publiés jusqu'à présent pour la seule année 2018, ce qui témoigne de la vitesse d'intérêt de la recherche récemment. Une analyse d'un champ agrégé de groupes de mots-clés créés à partir de l'ensemble des 2 520 documents montre que les principaux sujets d'intérêt de la R & D sont les crypto-devises, la sécurité des données, les applications et l'Internet des objets. L'Académie chinoise des sciences (49 publications), IBM (48) et le CSIRO australien (36) sont les principaux auteurs. Au Canada, l'Université de la Colombie-Britannique est l'entité la plus prolifique, avec 11 publications. Les principales organisations militaires du groupe de données sont l'Université nationale de technologie de défense de la Chine (19 publications), le laboratoire de recherche de l'US Air Force (11) et le laboratoire de recherche de l'armée américaine (5).

Selon la littérature, les applications potentielles de la technologie des registres distribués, en particulier les chaînes de blocs, semblent presque illimitées et devraient avoir un impact radical sur de nombreuses industries dans les années à venir. Pour les gouvernements, la TRD pourrait contribuer à rationaliser la prestation des soins de santé, améliorer la collecte des taxes, délivrer des passeports plus sûrs et, d'une manière générale, assurer l'intégrité des archives et des services gouvernementaux. Pour les organisations de défense et de sécurité, la technologie promet de renforcer la sécurité et l'efficacité des chaînes d'approvisionnement, de protéger les données et les communications sensibles et de permettre une gestion plus efficace des identités.
Cependant, malgré le récent enthousiasme et la montée en puissance des initiatives TRD à travers le monde, il reste encore à déterminer si la technologie répondra aux attentes élevées. Plusieurs obstacles et défis subsistent, tels que des problèmes de réglementation, des besoins en énergie et le fait qu'une chaîne de blocs sans devise locale soit viable ou que la TRD puisse fournir une meilleure solution que la technologie existante.