Blockchain Research and Applications: A Systematic Mapping Study

Sagar Bharadwaj K.S*, Samvid Dharanikota†, Adarsh Honawad‡ and K. Chandrasekaran §
Department of Computer Science and Engineering, National Institute of Technology Karnataka
Surathkal, Mangalore - 575025
Email: *sagarbharadwaj50@gmail.com, †samvid.dharani@gmail.com, ‡adarsh2397@gmail.com, §kchnitk@ieee.org

Abstract—**Brought to the limelight by the famous Bitcoin, blockchain has since evolved, and now sees a lot of use cases apart from cryptocurrencies, such as in distributed storage systems, finance, healthcare, and so on. It is, therefore, an area of scrutiny by a lot of researchers and application developers. Significant amount of research on blockchain involves application of blockchain technology to solve problems from various domains or improve the existing architecture of blockchain itself. The recent trend towards the decentralization of the Internet has given rise to many decentralized applications which also rely fundamentally on blockchain. In this paper, we conducted a systematic mapping study on blockchain technologies. The objective of the study is to identify and map various domains of research related to blockchain and recognize possible directions for future research. We do so by formulating a set of well-defined research questions and providing answers to them.**

Index Terms—**Blockchain, Systematic Mapping Study, Blockchain research, Blockchain applications**

I. INTRODUCTION

The blockchain is a distributed data storage ledger with certain key features that rely heavily on cryptography. This structure, which is replicated over all nodes in a network (dependent on the type of blockchain), is fundamentally a cryptographically linked chain of blocks, similar to a linked-list data structure. Each block, along with data, consists of a hash of the previous block in the chain, until the genesis block (the first block) whose hash field is 0.

This property ensures a key aspect of blockchain, immutability, in the following way: Assume the data in block n is being tampered with. This change would need to be followed by a recalculation of that block's hash, which is present in block number n+1. This would lead to re-computation of the hash of block n+1 and the following blocks until the latest block. This implies immutability because the creation of a new block in the network now becomes difficult (dependent on the blockchain protocol), leading to honest nodes which do not tamper with the data.

Blockchain also ensures privacy to an extent as the user identities are just cryptographic keys and not their information or credentials. Hence, user's personal details are not compromised in case of a breach. The blockchain is decentralized and so no single node manages the network and the blockchain itself. This fact eliminates any single-point-of-failure issues that centralized systems such as most of the current Internet technologies face.

It is to be noted that a blockchain is not complete without the network architecture that buttresses it, just as in any distributed system.

These properties of decentralization, immutability, and privacy make it an attractive architecture to be used in various use-cases.

Moreover, as a consequence of the distributed nature of the blockchain architecture, several issues that pertain to standard distributed systems such as consensus and consistency among others, also apply here. Moreover, because there is no one perfect solution to the issues in distributed systems, there is always scope for improvement concerning technologies surrounding blockchain.

This paper is a systematic mapping study of the work done in the area of blockchain. Several attempts [66] [4] have been made to prepare such studies earlier, but they are now outdated owing to the rapid progress in the research of blockchain systems. Furthermore, they have included only the papers that are openly accessible. Mapping the published literature, we highlight the areas in blockchain that are actively being researched and we also highlight the current and potential use-cases of blockchain.

Further, section 2 describes the research methodology that we have used in conducting our mapping study. We define the research questions that we attempt to answer and the motivation behind the same. In Section 3, we elaborate on basic publication related information such as the year of publication and types of publications obtained after our search process. Section 4 answers the defined research questions. Finally we present concluding remarks in Section 5.

II. RESEARCH METHODOLOGY

We have followed the standard procedure for a systematic mapping study, with minor changes as applicable, as defined in [46]. We have documented our entire search. procedure along with the results online [51]

A. Research Questions

The first step is to identify the research questions that are to be answered with this systematic mapping study. The questions have been identified and elaborated as follows:

RQ1: How have publication amount, frequency, and research topics changed over time?

This question seeks to answer how the trends in blockchain research have changed over time, from its inception with the Bitcoin. We seek to identify areas of research in blockchain that are growing and the areas that are gradually being

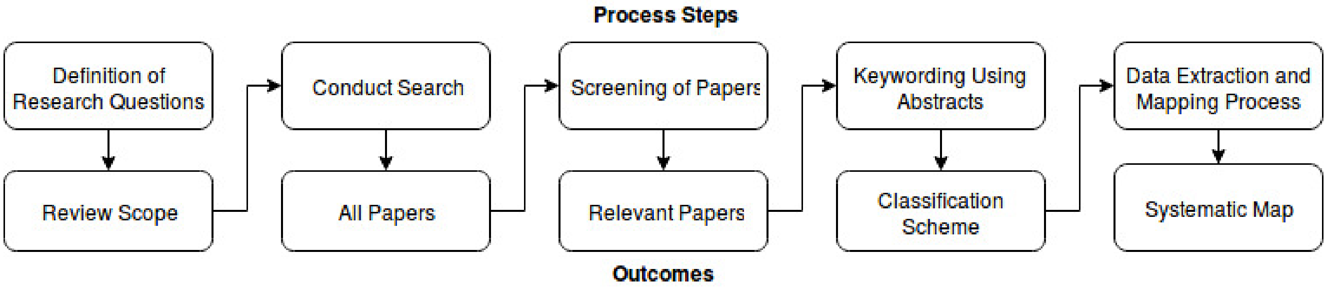

Fig. 1. Research Methodology[46]

ignored by answering this research question.

RQ2: What are the use-cases of blockchain technology?

Blockchain is seeing applications in a wide variety of use-cases beyond Cryptocurrencies, for which it was designed initially, especially with the shift towards the decentralized web. The answer to this question will outline the domains in which blockchain is being used, providing solutions to the problems in those areas.

RQ3: What are the areas of current research in blockchain?

While RQ2 focuses on the domains where blockchain is used, RQ3 aims to elaborate on enhancements and optimizations that are being made to blockchain architectures themselves. Blockchain architectures in the current scenario are not perfect and have many drawbacks in terms of scalability and transaction processing speed, among others, and this question addresses the work done towards improvement in these aspects.

RQ4: How is research on blockchain distributed geographically?

We aim to provide an estimate of the number of papers published in different countries. The answer to this research question enables one to study where in the world blockchain research is being carried out.

RQ5: What is the future research direction for blockchain?

This question aims to draw conclusions from the above questions and predicts where the research in blockchain is heading towards, and the areas researchers are most likely to pursue. We also intend to point out some areas of research that were lacking attention at the onset of blockchain but are now significant areas of research.

B. Selection of Paper Sources

Our aim was to select popular sources that would contain the most significant number of publications. IEEE Explore, ACM Digital Journal, SpringerOpen, and ScienceDirect were considered owing to having an extensive collection of papers in the blockchain domain. Springer, although as popular as the above databases, was not considered because searching for the keyword 'blockchain' resulted in only book chapters and irrelevant papers.

C. Conducting the Search

The second stage of the systematic mapping study is to form the search strings that are used for the search of the papers and to conduct the search. The search strings that we used to obtain results from different sources can be found at [51].

In our database search process, only those publications having the keyword 'blockchain' in their title or keywords section were selected. This eliminates the consideration for papers that do not have the word in either field but refer to the same in the content of the paper.

D. Screening of Relevant Papers

We then applied filters on the paper databases to extract only journal and conference papers. We selected only those sources that are peer-reviewed. Following the database filtering, we screened the papers first based on their titles and then abstracts and further excluded/included papers based on a set of inclusion and exclusion criteria:

Exclusion Criteria:

- Review/Summary/Secondary papers - these papers do not pertain to the scope of a Systematic Mapping Study and hence were removed
- Book chapters/Keynotes/Case studies/Work-in-progress/ News articles papers - for the same reason as above
- Duplicate papers
- Papers where blockchain is not the main area of focus
- Papers that focus on an economic/financial point of view
- Papers that address issues pertaining to a specific country and do not focus on generic issues
- Papers not written in the English Language
- Commentaries/News

Inclusion Criteria:

- Papers that introduce novelty in blockchain
- Papers that explained the use of blockchain in other domains
- Papers that enhance blockchain

Due to the large number of papers published on blockchain, we had to stick to rigorous filtering criteria to reduce the number of papers for efficient classification. There is a possibility that we may have missed out some relevant papers.

Table I shows the number of research papers that we considered initially and the number of papers left at the end of application of the corresponding filtering criteria.

E. Data Extraction and Mapping

After filtering relevant and vital papers, we have identified categories that each of the papers belongs to, by reading their abstracts. The list of these classifications, along with the papers that belong to these classifications are listed in [51]. There are a total of 123 categories that we have identified. We have classified the chosen 604 primary papers under these 123 categories. Several papers were found to belong to multiple categories. Compared to [66], which has classified a total of 41 primary papers into 14 classifications, our mapping study is done on a much larger scale owing to the rapid increase in research on blockchain technologies.

III. PUBLICATION STATISTICS

Papers obtained after all filtering criteria were applied were analyzed to give the following inferences.

A. Search and Selection Results

The search string that was formed based on the relevant keywords and exclusion criteria was used for searching on the various publications sites. The results were obtained with details like title, abstract, keywords, authors, citations and other vital details. We began the work on title screening. We excluded several papers marked as Demos and Tutorials. We also found several papers with single pages, which do not have any significant contributions or citations and hence removed them. We also went through the abstracts of each paper that cleared the title screening phase and identified review papers, secondary papers like literature surveys and papers that don't focus on blockchain. We removed such papers from consideration. The first phase of the classification of papers was also done along with the abstract screening phase. After title screening, abstract screening, and duplicate removal phases, we had a total of *604* primary papers that we could consider for the purpose of this Systematic mapping study.

B. Publication Year

Blockchain research started gaining its popularity in the year 2015 (according to publication searches). Between 2015 to 2018, the number of papers in the domain of blockchain has risen significantly. One of the attributes of this rise is due to the advent of newer blockchain technologies that are more capable than Bitcoin [42] in factors like transaction speed, storage and the ability to execute code.

With the increase in such factors, the scope of blockchain has broadened and today blockchain is being used in several areas like healthcare, supply chain, edge computing, education apart from just finance. One notable example would be the Ethereum blockchain [63]. Ethereum was proposed in 2014 and brought with it the ability to execute user-defined Turing complete code, called Smart Contracts. With this Ethereum swept its way into several Internet of Things (IoT) based applications. Smart Contracts were then utilized in several other domains like healthcare, energy market and vehicular networks.

Figure 2 gives a count of the publications with respect to the year of publication after applying all the filtering criteria.

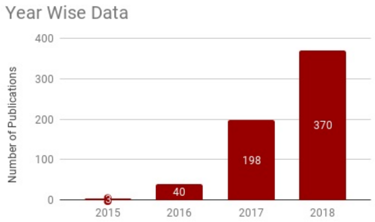

Fig. 2. Year of Publication

C. Publication Type

These numbers were obtained after the application of all the filtering criteria. Figure 3 shows the count of papers obtained from the different publication types. Papers presented in workshops and symposiums have been included under conference.

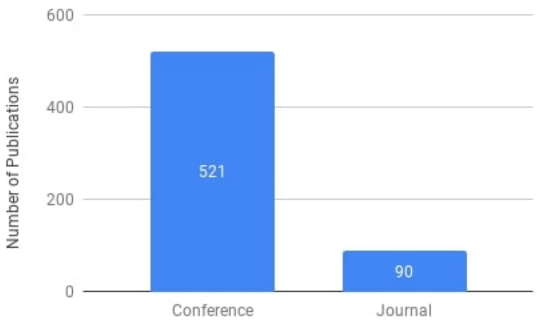

Fig. 3. Papers classified according to Publication Type

IV. DISCUSSION

Based on the results of our search, we answer the research questions posed above:

TABLE I
KEYWORD SEARCH RESULTS

Filtering Phase	IEEE	ACM Digital Journal	Science Direct	Springer Open	Total
Conducting the Search	820	279	183	43	1325
Search Filters applied	773	251	116	43	1183
Title Screening	639	198	62	22	921
Abstract Screening	421	135	45	10	611
Duplicate Removal	–	–	–	–	604

A. RQ1: How have publication amount, frequency, and research topics changed over time?

Figure 2 shows the rapid growth in number of publications related to blockchain technology over time. We analyzed the relative percentages of research areas in each year, i.e how much of the total research in a particular year is conducted in different research fields. In the earlier mapping study on blockchain technologies [66], most of the research was focused on the enhancement of Bitcoin. Around 80.5% of all the papers studied in [66] have focused on Bitcoin. However, the research scenario is largely different today and the applications of blockchain have diversified.

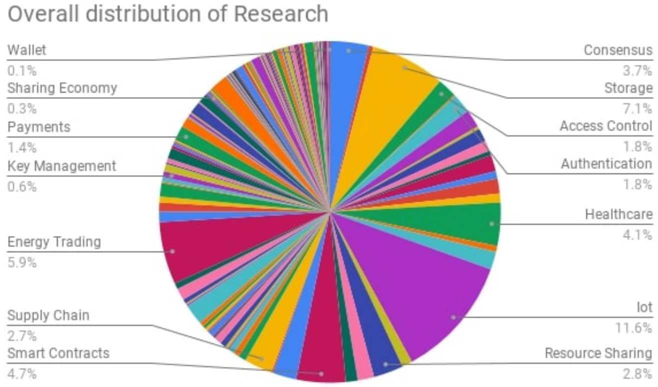

Fig. 4. Distribution of Research areas in Blockchain

Figure 4 shows a pie chart of relative percentages of publications classified under each of the research areas. The complete data and list of all the categories or research areas are published in [51]. Compared to [66], this represents a wide range of research possibilities. We also analyzed how blockchain research areas have evolved over time.

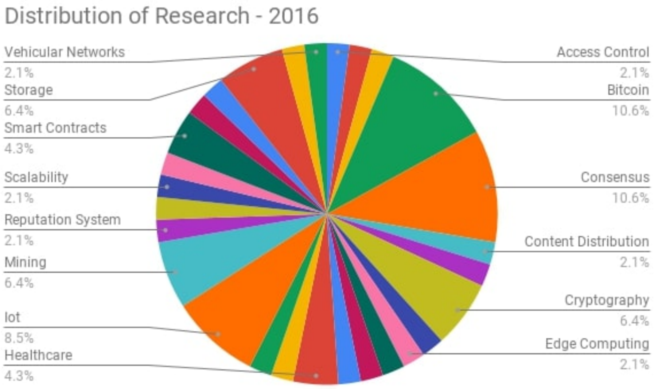

Fig. 5. Distribution of Research areas in Blockchain - 2016

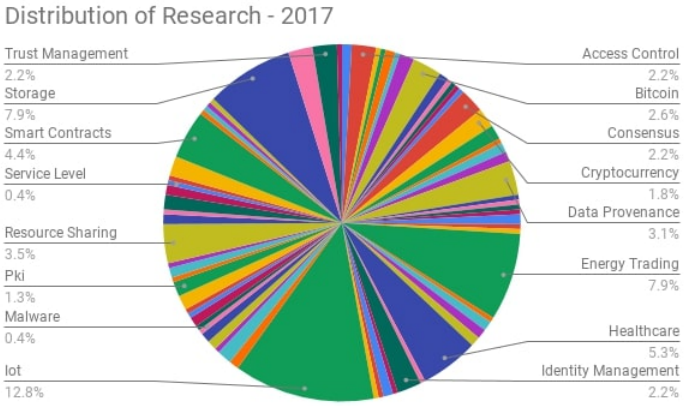

Fig. 6. Distribution of Research areas in Blockchain - 2017

Figure 5, Figure 6 and Figure 7 represent the evolution of research areas over time. Many inferences about the evolution of research in blockchain can be drawn based on the data presented in these charts. Bitcoin was a major area of research spanning over 80.5% of all publications during the onset of blockchain research [66]. Bitcoin occupied 10.6% of all research in blockchain in 2016 owing to a boom in the potential applications of blockchain. This percentage reduced to 2.6% in 2017 and is less than 1% in 2018. This not only shows a shift of attention away from Bitcoin oriented research but also points to the increased efforts put into generalizing the applications of blockchain. Another interesting result is the evolution of application of blockchain in the IoT. [9] summarised different methods of adopting blockchain in the IoT domain and the number of publications have gone up ever since. The application of blockchain in IoT occupied 8.5% of the total blockchain research in 2016. In 2018, research in blockchain and IoT increased to 11.3%. With the increase in the total number of papers published. This shows that blockchain and IoT combination is one area which researchers are actively looking at. The number of research areas has also risen significantly since 2016 as shown by the number of segments in the Pie charts (4). Many new areas like Energy

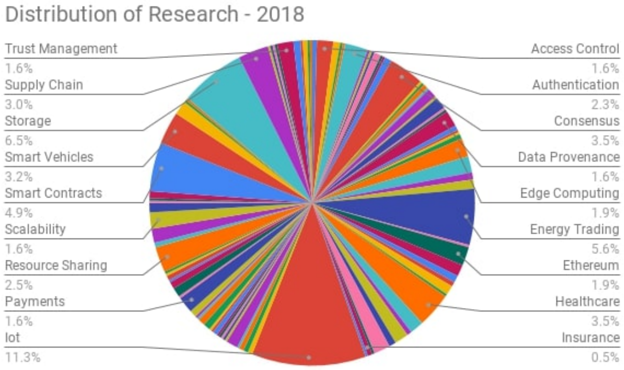

Fig. 7. Distribution of Research areas in Blockchain - 2018

trading on smart grid occupy a significant portion of research today.

B. RQ2 : What are the use-cases of blockchain technology?

From the various areas where blockchain is being used today, IoT stands above them all (11.6% of the papers) followed by Storage solutions (7.1%) and Energy Trading (5.9%). This is followed by other domains like Healthcare (6.6%) and Smart grids (5.7%). Blockchain aids applications in these domains by enhancing fundamental features which includes authenticity, security, data integrity, data immutability, data privacy, data provenance, and data ownership among many others.

We have chosen some papers in certain important domains, and we provide a gist of the research conducted in each of those domains. All the papers mentioned in this section are referred to by their IDs in [51].

There has been a significant amount of research happening in the fields of IoT and blockchain, paving the way to many possibilities. In our study we found 82 papers that directly deal with a combination of blockchain and IoT. [P160][44] shows how blockchain can be used for access management in IoT scenarios. While current centralized methods do exist, scalability of such methods is limited. Blockchain with its distributed access control system for IoT seems to provide a new and better alternative. [P219][22] uses blockchain as a method to build trust in consumers to trade their smart devices' data for incentives. They describe how the IoT device will be sold to a user by proving the devices integrity without a third-party and provide a secure method of sharing the users data. However, blockchain remains computationally expensive and one such paper [P561][12] tackles the problem by introducing an optimized blockchain. The main idea is to create an overlay network of high resource devices to handle the blockchains operations while still providing end-to-end security and privacy to the low resource IoT devices.

Smart Grid is vital in today's world to increase distribution of locally produced energy, mostly renewable energy. However, a centralized architecture often poses issues of reliability and privacy or anonymity. In our study, we found a total of 43 papers directly dealing with Energy trading through blockchain transactions. A blockchain based integration into the energy trading society has been proposed successfully by [P505][3]. [P196][41] offers a blockchain and smart contracts solution to tackle distribution of energy from multiple sources and allows to handle payments securely.

Several blockchain based solutions have been proposed to tackle problems related to data storage on the cloud. [P461][33] introduces ProvChain which is an architecture to embed provenance data into blockchain transactions. Most of the storage solutions use blockchain architecture as middleware between users of the data and the data itself to enhance several features of the system including privacy, security, data provenance, auditing capabilities, anonymity and so on. [69] was one of the early papers to give details on the way a blockchain layer can provide enhanced privacy in storage systems. In our study, we have collected 51 papers that utilize blockchain as a storage solution.

Edge computing is used to offload computation required for mining onto edge devices, from mobiles, enabling mobile systems to participate in the blockchain network [P376][35]. There are also pricing schemes designed for Edge Service Providers (ESPs) [P429][64]. Edge nodes also make use of distributed control systems, which in turn have function blocks as their main component. Smart contracts are used to implement these function blocks [P141][57]. Blockchain is also used for trusted data sharing between edge nodes. Ideas are also proposed to reduce work done by mining to replace Proof-of-Work by a Proof-of-Collaboration, catering to the limited computational and storage resources of edge devices.

Blockchains can also replace a traditional CA, as proposed by [P22][65]. Additional x509 certificate extensions are proposed which facilitate smart contracts to handle the tasks of a CA such as issuing, storing, validating and revoking certificates. A particular application of blockchain in verification of certificates for SSL/TLS secured communication is proposed in [P212][8]. A distributed PKI is proposed in [P211][49] which supports a distributed certificate library, where the miners in the blockchain environment act as CAs, ensuring the correctness of certificates. Smart contacts have also been used to implement a dynamic trust protocol in PKIs [P592][2]. [P338][59] proposes a novel approach of creating a cloud-based PKI using blockchain, where certificate issuing is done on the cloud, and the blockchain is used to record the issued certificates.

We came across several unique use cases of blockchain during our studies. For example [P286][50] deals with Mixed Reality Applications. [P276][62] uses blockchain in a

Transaction Processing System. [P201][18] uses blockchain in a video surveillance system. [P266][43], [P360][26], [P93][55] use blockchain to collect and analyze data related to Pollution. [P477][37], [P486][25] use blockchain as a reviews framework. [P155][52] uses blockchain to record work history of employees and aids in Corporate Management. [P138][48], [P388][23], [P467][67], [P77][34], [P95][24] deal with Electric vehicles and charging stations. [P413][20], [P512][14], [P521][53] use blockchain as a framework to enhance Information Technology Operations (Ops). A list of all the categories and the corresponding papers for each category can be found at [51].

C. RQ3: What are the areas of current research in blockchain technology?

While blockchain is used in many domains as seen above, there has been intense research going on to enhance blockchain technology itself. In our study, we identified several papers that deal exclusively with generic blockchain. These papers do not narrow down on a specific use case or a domain but focus on features such as blockchain's storage scalability, transaction scalability, consensus protocols, formal analysis of blockchain and so on. Figure 8 shows relative percentages of papers according to their primary focus.

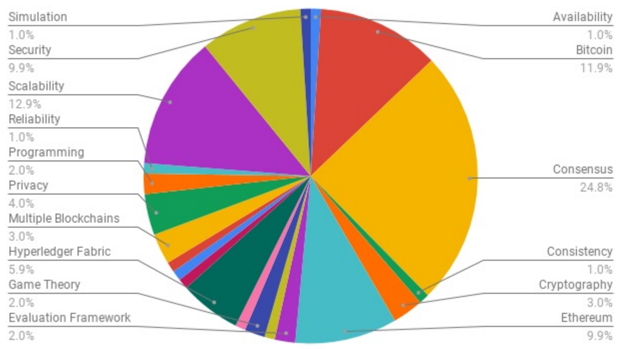

Fig. 8. Distribution of research on generic blockchain

We found a total of 26 papers dealing with consensus algorithms. In a decentralized system, we need algorithms to reach consensus among the participating nodes. Bitcoin, one of the first useful implementation of blockchain uses the Proof of Work consensus algorithm. However, this algorithm is computationally expensive and faces several security threats. Efforts have been made to come up with new consensus algorithms like Proof of Luck, Proof of Stake, Proof of Trust and even improvements on existing consensus algorithms. [P453][40] describes the Proof of Luck method of consensus in Trusted Execution Environments. The idea is to use a random number generator to pick a consensus leader, offering equitably distributed mining with lower latency and energy consumption. [P52][54] attempts to solve the 51% majority attack on the Bitcoin network by proposing a modified Proof of Work consensus algorithm.

[P252][61], [P429][64] and [P610][68] model blockchain from a Game Theoretic perspective to prove the robustness and security features of some blockchain based solutions. [P252][61] model their content caching system based on blockchain as a Chinese restaurant game and analyze the Nash equilibrium of the game. [P429][64] model the Edge Computing service provider as a Stackelberg game. There have not been many studies conducted on rigorous mathematical proofs to prove security and safety properties that blockchain based solutions claim to offer. [P335][15], [P336][1] focus on formal verification of these properties. [P416][10], [P516][45] discuss alternate solutions for programming languages that can be used on blockchain. Currently, Ehtereum uses solidity as the primary Programming language to write smart contracts [11]. [P416][10] proposes a language named Obsidian which the authors claim to be safer than Solidity. [P516][45] propose Simplicity, a typed, combinator-based, functional language without loops and recursion to be used in blockchain based applications.

Ethereum is one of the most widely used platforms not just by Decentralised Application developers but also researchers to test their ideas. [P313][5] proposes a query language specific to the Ethereum blockchain based on SQL. This was proposed to extract transaction and block details in the Ethereum blockchain and filter them based on transaction details within the block. Ethereum specific research is also done in [P394][21] where a tool is proposed to analyze Ethereum smart contracts for out-of-gas vulnerabilities wherein a Smart Contract's balance is locked permanently if it terminates abruptly when it runs out of gas, and this abrupt abortion is not handled properly.

In addition to this, several papers are dealing with issues of storage scalability, computational requirements, faster and scalable consensus algorithms.

D. RQ4: How is research on blockchain distributed geographically?

Figure 9 shows the comparison amongst the different countries where blockchain based research papers have originated. The research is being significantly carried forward by universities and industries in China (23.9%) and USA (13.6%) while all other countries have a contribution of less than 5%.

China seems to be the current hot spot for blockchain research. Blockchain research in China is encouraged by several dominant institutions including the communist party, central bank, supreme people's court and the Bank of China [16]. Several strategic reasons for significant blockchain research in China has been described in [16].

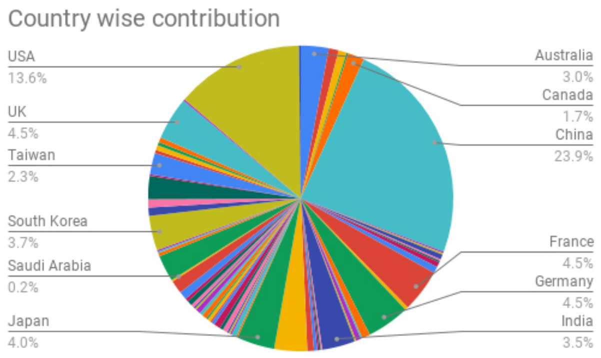

Fig. 9. Research Papers classified according to the Country

E. RQ5 : What are the possible directions for future blockchain research?

The previous research question focused on the current research areas in blockchain. We identify some possible future research areas related to blockchain by identifying the most popular fields that researchers are working on by conducting a search for literature in very recent years (2017 and 2018). This section reviews these research areas by providing a comprehensive overview of the identified fields.

Scalability of blockchains has been a burgeoning area of research interest. In the initial stages of blockchain that was popularised by Bitcoin [42], blockchain consensus algorithms like proof-of-work focused on scalability with respect to the number of nodes. However, as the number of transactions on the Bitcoin increased, there began considerable work on increasing the throughput of the Bitcoin network. Some early work includes Bitcoin-NG [17] which uses Proof-of-work to elect a leader and allows it to add micro-transactions in the inter mining period. The GHOST rule [56] proposed a new conflict resolution method in proof-of-work mining that makes it safer to increase the block mining frequency, thereby increasing scalability in terms of the number of transactions. Replacing a linear chain of blocks with DAG (Directed Acyclic Graphs), another method was introduced by [30] to include all mined blocks in the log if they are not conflicting.

Bitcoin lightning network [47] propose the creation of micropayment channels between two concerned parties to increase scalability by deferring broadcasting transactions to the rest of the blockchain network. Sharding of blockchain has also been proposed as a solution for the scalability problem. Sharding involves different nodes handling different subsets of the blockchain. ELASTICO [36] proposed a sharding algorithm that works in the presence of Byzantine failures. Sharding increases the throughput of the network linearly with respect to the computational power of the network. However, sharding reduces the security provided by the system making it susceptible to attacks as it reduces the number of attackers required to introduce compromised data into the blockchain network. Omniledger [28] proposes solutions to maintain security in a sharded blockchain. Recent solutions include using inspector nodes [7] to reshuffle validator nodes when required to reduce reshuffling overhead. Polyshard [31] claims to introduce scalability in terms of Security, Storage efficiency and Throughput by using a ”polynomially coded sharding” scheme.

Another area of potential future research seems to be the design of consensus algorithms. A change in consensus algorithms can also result in scalable blockchains. [58] details how expensive consensus mechanisms are not needed in permissioned systems, thereby allowing usage of consensus mechanisms that are known to be scalable in terms of performance. Vukolić in [60] has compared proof-of-work and BFT protocols with respect to scalability. Many blockchain solutions use Byzantine Fault Tolerant [29] protocols to construct scalable blockchains. However such blockchains are not scalable with respect to the number of nodes because of the large number of messages exchanged between nodes. There has been some work done to reduce communication overheads in BFT. Many BFT protocols modeled after Practical Byzantine Fault Tolerance [6] have been used as consensus protocols in blockchain. Stellar Consensus Protocol [38] introduces Federated Byzantine Agreement (FBA), removing the need for nodes to presuppose a unanimously accepted membership list. Algorand [19] proposes a novel Byzantine Agreement (BA) protocol to reach consensus among users. The core of Algorand uses a protocol called BA* that scales to many users, offers reduced latency and ensures strict safety rule by making sure there are no forks in the blockchain. Ouroboros [27] is a Proof-of-stake based consensus algorithm where the authors have proved that honest behavior is a Nash equilibrium, thus proving that attacks are quickly neutralised.

Combination of blockchain with IoT, as suggested by our search results, is being considered as one of the most lucrative fields to work. [9] has summarized the usability of blockchain in IoT. Research on blockchain with IoT parallels research on decentralized smart energy grids. There have been some solutions to enable Peer-to-Peer energy trading among devices in an Industrial IoT setup. [32] exploits a consortium blockchain to provide a secure energy trading mechanism. Energy markets where trading of locally produced renewable energy can take place without interference by an intermediary have been proposed and tested [39]. Blockchains are being used for communication between smart home devices [13]. An appropriate combination of blockchain, multi-signatures, and anonymous encrypted message propagation schemes can be used to build a decentralized smart energy grid system that provides increased security and privacy in comparison to centralized systems [3].

V. CONCLUSIONS

This paper aims to provide an overall idea of the domains where blockchain has been used to resolve existing issues or provide new innovative solutions. Through our screening process, we selected a set of 604 primary papers to conduct our mapping study. We have provided a broad classification of the areas under which work done can be classified. We have included statistical data regarding the number of papers published in each category, type of publication (Journal, Conference) and country of origin of the research. We included year-wise distribution of the various domains of blockchain research to better understand the change in research over the years. To further understand the research, we selected a few popular papers under the significant classifications and provided a gist about the type of work being carried out in the domain. We attempted to answer all the Research Questions that have been formulated. We have documented the entire process and published our results online for verification [51].

The frequency at which papers are being published is very high. The same search conducted a few weeks after the publication of this paper may lead to different results than what we have obtained. This is an inevitable drawback. However, we believe that this study will give researchers, both experienced and new, an idea about the work done so far.

REFERENCES

[1] Tesnim Abdellatif and Kei-Léo Brousmiche. Formal verification of smart contracts based on users and blockchain behaviors models. In *New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on*, pages 1–5. IEEE, 2018.

[2] Abu Shohel Ahmed and Tuomas Aura. Turning trust around: Smart contract-assisted public key infrastructure. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 104–111. IEEE, 2018.

[3] Nurzhan Zhumabekuly Aitzhan and Davor Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852, 2018.

[4] Maher Alharby and Aad van Moorsel. Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372*, 2017.

[5] Santiago Bragagnolo, Henrique Rocha, Marcus Denker, and Stéphane Ducasse. Ethereum query language. In *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, pages 1–8. ACM, 2018.

[6] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OSDI*, volume 99, pages 173–186, 1999.

[7] Anamika Chauhan, Om Prakash Malviya, Madhav Verma, and Tejinder Singh Mor. Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 122–128. IEEE, 2018.

[8] Jing Chen, Shixiong Yao, Quan Yuan, Kun He, Shouling Ji, and Ruiying Du. Certchain: Public and efficient certificate audit based on blockchain for tls connections. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 2060–2068. IEEE, 2018.

[9] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *Ieee Access*, 4:2292–2303, 2016.

[10] Michael Coblenz. Obsidian: a safer blockchain programming language. In *Proceedings of the 39th International Conference on Software Engineering Companion*, pages 97–99. IEEE Press, 2017.

[11] Chris Dannen. *Introducing Ethereum and Solidity*. Springer, 2017.

[12] Ali Dorri, Salil S Kanhere, and Raja Jurdak. Towards an optimized blockchain for iot. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pages 173–178. ACM, 2017.

[13] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, pages 618–623. IEEE, 2017.

[14] Jun Duan, Alexei Karve, Vugranam Sreedhar, and Sai Zeng. Service management of blockchain networks. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 310–317. IEEE, 2018.

[15] Zhangbo Duan, Hongliang Mao, Zhidong Chen, Xiaomin Bai, Kai Hu, and Jean-Pierre Talpin. Formal modeling and verification of blockchain system. In *Proceedings of the 10th International Conference on Computer Modeling and Simulation*, pages 231–235. ACM, 2018.

[16] Steven Ehrlich. Making sense of china's grand blockchain strategy, 2018. https://www.forbes.com/sites/stevenehrlich/2018/09/17/making-sense-of-chinas-grand-blockchain-strategy/75772ce23678.

[17] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In *NSDI*, pages 45–59, 2016.

[18] Pierluigi Gallo, Suporn Pongnumkul, and Uy Quoc Nguyen. Blocksee: Blockchain for iot video surveillance in smart cities. In *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, pages 1–6. IEEE, 2018.

[19] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, pages 51–68. ACM, 2017.

[20] Roman Graf and Ross King. Neural network and blockchain based technique for cyber threat intelligence and situational awareness. In *2018 10th International Conference on Cyber Conflict (CyCon)*, pages 409–426. IEEE, 2018.

[21] Neville Grech, Michael Kong, Anton Jurisevic, Lexi Brent, Bernhard Scholz, and Yannis Smaragdakis. Madmax: Surviving out-of-gas conditions in ethereum smart contracts. *Proceedings of the ACM on Programming Languages*, 2(OOPSLA):116, 2018.

[22] Thomas Hardjono and Ned Smith. Cloud-based commissioning of constrained devices using permissioned blockchains. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pages 29–36. ACM, 2016.

[23] Xiaohong Huang, Cheng Xu, Pengfei Wang, and Hongzhe Liu. Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access, vol. PP*, (99):1–1, 2018.

[24] Xiaohong Huang, Yong Zhang, Dandan Li, and Lu Han. An optimal scheduling algorithm for hybrid ev charging scenario using consortium blockchains. *Future Generation Computer Systems*, 91:555–562, 2019.

[25] Zeeshan Jan, Allan Third, Luis-Daniel Ibanez, Michelle Bachler, Elena Simperl, and John Domingue. Sciencemiles: Digital currency for researchers. In *Companion of the The Web Conference 2018 on The Web Conference 2018*, pages 1183–1186. International World Wide Web Conferences Steering Committee, 2018.

[26] Khamila Nurul Khaqqi, Janusz J Sikorski, Kunn Hadinoto, and Markus Kraft. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Applied Energy*, 209:8–19, 2018.

[27] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer, 2017.

[28] Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. Omniledger: A secure, scale-out, decentralized ledger. *IACR Cryptology ePrint Archive*, 2017:406, 2017.

[29] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[30] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. Inclusive block chain protocols. In *International Conference on Financial Cryptography and Data Security*, pages 528–547. Springer, 2015.

[31] Songze Li, Mingchao Yu, Salman Avestimehr, Sreeram Kannan, and Pramod Viswanath. Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously. *arXiv preprint arXiv:1809.10361*, 2018.

[32] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3690–3700, 2018.

[33] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pages 468–477. IEEE Press, 2017.

[34] Chao Liu, Kok Keong Chai, Xiaoshuai Zhang, Eng Tseng Lau, and Yue Chen. Adaptive blockchain-based electric vehicle participation scheme in smart grid platform. *IEEE Access*, 2018.

[35] Mengting Liu, F Richard Yu, Yinglei Teng, Victor CM Leung, and Mei Song. Joint computation offloading and content caching for wireless blockchain networks. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 517–522. IEEE, 2018.

[36] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 17–30. ACM, 2016.

[37] Daniel Martens and Walid Maalej. Reviewchain: Untampered product reviews on the blockchain. *arXiv preprint arXiv:1803.01661*, 2018.

[38] David Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015.

[39] Esther Mengelkamp, Benedikt Notheisen, Carolin Beer, David Dauer, and Christof Weinhardt. A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science-Research and Development*, 33(1-2):207–214, 2018.

[40] Mitar Milutinovic, Warren He, Howard Wu, and Maxinder Kanwal. Proof of luck: An efficient blockchain consensus protocol. In *Proceedings of the 1st Workshop on System Software for Trusted Execution*, page 2. ACM, 2016.

[41] Eric Münsing, Jonathan Mather, and Scott Moura. Blockchains for decentralized optimization of energy resources in microgrid networks. In *Control Technology and Applications (CCTA), 2017 IEEE Conference on*, pages 2164–2171. IEEE, 2017.

[42] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[43] Sina Rafati Niya, Sanjiv S Jha, Thomas Bocek, and Burkhard Stiller. Design and implementation of an automated and decentralized pollution monitoring system with blockchains, smart contracts, and lorawan. In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–4. IEEE, 2018.

[44] Oscar Novo. Blockchain meets iot: an architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 2018.

[45] Russell O'Connor. Simplicity: a new language for blockchains. In *Proceedings of the 2017 Workshop on Programming Languages and Analysis for Security*, pages 107–120. ACM, 2017.

[46] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. Systematic mapping studies in software engineering. In *EASE*, volume 8, pages 68–77, 2008.

[47] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. *See https://lightning. network/lightning-network-paper. pdf*, 2016.

[48] Matevz Pustisek, Andrej Kos, and Urban Sedlar. Blockchain based autonomous selection of electric vehicle charging station. In *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, pages 217–222. IEEE, 2016.

[49] Bo Qin, Jikun Huang, Qin Wang, Xizhao Luo, Bin Liang, and Wenchang Shi. Cecoin: A decentralized pki mitigating mitm attacks. *Future Generation Computer Systems*, 2017.

[50] Bektur Ryskeldiev, Yoichi Ochiai, Michael Cohen, and Jens Herder. Distributed metaverse: Creating decentralized blockchain-based model for peer-to-peer sharing of virtual spaces for mixed reality applications. In *Proceedings of the 9th Augmented Human International Conference*, page 39. ACM, 2018.

[51] Samvid Sagar, Adarsh. *Systematic Mapping Study on Blockchain research*, 2018. https://goo.gl/xSUC1i.

[52] Paul Sarda, Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, and Jun Han. Blockchain for fraud prevention: A work-history fraud prevention system. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 1858–1863. IEEE, 2018.

[53] Tatsuya Sato and Yosuke Himura. Smart-contract based system operations for permissioned blockchain. In *New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on*, pages 1–6. IEEE, 2018.

[54] Ning Shi. A new proof-of-work mechanism for bitcoin. *Financial Innovation*, 2(1):31, 2016.

[55] Dong-Her Shih, Po-Yuan Shih, and Ting-Wei Wu. An infrastructure of multi-pollutant air quality deterioration early warning system in spark platform. In *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pages 648–652. IEEE, 2018.

[56] Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 507–527. Springer, 2015.

[57] Alexandru Stanciu. Blockchain based distributed control system for edge computing. In *Control Systems and Computer Science (CSCS), 2017 21st International Conference on*, pages 667–671. IEEE, 2017.

[58] Tim Swanson. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. *Report, available online, Apr*, 2015.

[59] Hitesh Tewari, Arthur Hughes, Stefan Weber, and Tomas Barry. X509cloudframework for a ubiquitous pki. In *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*, pages 225–230. IEEE, 2017.

[60] Marko Vukolić. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In *International Workshop on Open Problems in Network Security*, pages 112–125. Springer, 2015.

[61] Wenbo Wang, Dusit Niyato, Ping Wang, and Amir Leshem. Decentralized caching for content delivery based on blockchain: A game theoretic perspective. *arXiv preprint arXiv:1801.07604*, 2018.

[62] Yunsen Wang and Alexander Kogan. Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30:1–18, 2018.

[63] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32, 2014.

[64] Zehui Xiong, Shaohan Feng, Dusit Niyato, Ping Wang, and Zhu Han. Optimal pricing-based edge computing resource management in mobile blockchain. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.

[65] Alexander Yakubov, Wazen Shbair, Anders Wallbom, David Sanda, et al. A blockchain-based pki management framework. In *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018*, 2018.

[66] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?a systematic review. *PloS one*, 11(10):e0163477, 2016.

[67] Tianyang Zhang, Himanshu Pota, Chi-Cheng Chu, and Rajit Gadh. Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency. *Applied Energy*, 226:582–594, 2018.

[68] Yang Zhen, Miao Yue, Chen Zhong-yu, Tang Chang-bing, and Chen Xin. Zero-determinant strategy for the algorithm optimize of blockchain pow consensus. In *Control Conference (CCC), 2017 36th Chinese*, pages 1441–1446. IEEE, 2017.

[69] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.