Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

A Survey On Security And Privacy In Blockchain And Software Defined Network

Mrs. G.Indumathi[1] , Dr. B.S.E.Zoraida[2]

[1]Research Scholar, Department of Computer Science, Bharathidasan University Kajamalai campus, Tiruchirappalli-23.

[2]Research Supervisor & Assistant Professor, Department of Computer Science, Bharathidasan University Kajamalai campus, Tiruchirappalli-23.

Abstract

Software-Defined Networking, more commonly referred to as software-defined networking (SDN), is a prospective new network paradigm that has developed as a response to the unprecedented development in the complexity of network management and configuration. Software-Defined Networking is also sometimes referred to as software-defined networking (SDN). Networking is the term that has been given to describe this paradigm. Software-defined networking, usually known as SDN for short, is a movement that attempts to make network operations and design more agile while also increasing the usability of core organisational components like routers and switches. The SDN project has several major aims, one of the most important of which is to disconnect the control plane from the data plane. Because of software-defined networking, commonly referred to as SDN, the knowledge and experience of the organisation has been combined into a software substance known as an SDN regulator. Because of this, network chairs are given the ability to gradually manage, safeguard, and develop network assets, as well as automatically shape the traffic design for the whole business. Even though SDN has introduced many fantastic new improvements to the architecture of the arrange, it also presents new security concerns and encourages diverse execution systems to disperse attack vectors, both of which have the potential to be problematic. SDN has brought many fantastic improvements to the architecture of the arrange. In this piece, a comprehensive illustration of how the Blockchain technology might be utilised to acquire and ensure SDN design is provided. In addition, the essay investigates the potential for combining the groundbreaking developments of software-defined networking (SDN) with blockchain technology in order to provide network architecture that is compliant with regulations, secure, and easy to use.

Index Terms: edge computing, network, Blockchain, storage, SDN.

Introduction

The properties of decentralization, peer-to-peer communication, and immutability that blockchain technology offers have contributed to an uptick in interest in the technology over the course of the past year. A digital ledger that is accessible to the general public and may be viewed by anybody who is currently connected to the network. The concept was initially proposed by Santoshi Nakamoto in 2008, when he presented the concept of the Bitcoin cryptocurrency. Since that point in time, more than 20,000 additional cryptocurrencies have been established, and

there are currently more than 20,000 of those cryptocurrencies available on the market.

despite the fact that Bitcoin use is not yet commonplace in most parts of the world. There are many different problems that are associated with Bitcoin, some of which include anti-money laundering (AML), the performance of legal and illegitimate mining, and other problems. It takes around seven to eight minutes for the mining process and the validation of the transaction to be completed in the Bitcoin system.

This idea is applicable to a wide variety of different application domains, some of which are healthcare, the Internet of Things (IoT), industry, and supply chain management, to mention just a few of those subfields. From an academic point of view, the primary emphasis of this investigation has been an examination of the many ways in which Blockchain technology has been put into practise in a variety of different application fields. The survey was carried out by the Blockchain Research Institute. In addition, current advancements that have been achieved by a range of organizations in order to implement the Blockchain approach in a variety of different domains have also been taken into consideration. In today's environment, the transfer of digital information from one end to the other is carried out over a transmission channel that cannot be relied upon. This makes the transmission of digital information vulnerable to attack. When it comes to this topic, keeping one's privacy and being anonymous are of the biggest significance. The technology that underpins blockchain makes it possible for people to directly communicate in an encrypted format. The decentralized ledger technology known as blockchain makes the details of all transactions openly accessible for viewing. However, once a transaction has been recorded, it cannot be altered in any way.

After conducting an in-depth analysis of the pertinent published research, it was found that blockchain technology is being implemented in a broad variety of significant application sectors. It should be noted that Blockchain is a probabilistic state machine, and that this fact renders it inappropriate for implementation in circumstances when it is necessary to arrive at decisions that are definitive. The provided an explanation of some of the possible applications of Blockchain technology and highlighted the ways in which Blockchain technology may be used to solve a variety of problems that are traditionally associated with databases. In addition, the highlighted the ways in which Blockchain technology may be used to improve the security of cryptocurrency transactions. Table 1 presents a comparison of the many different kinds of study that have been carried out on the Blockchain technology. This table may be found at the beginning of this article for your convenience. The technology behind blockchain is now one of the most competitive research sectors; yet, it does not yet have the necessary technological particulars to become truly employed in almost any business. The research papers are arranged in accordance with the numerous applications that can be developed from them.

S. No	Survey Papers	Year	Focus Area	Security Issue	Remarks
1.	**Xiaoqi Li**	**2017**	**Specific IoT**	**Covered**	**Conducted a security audit and located the actual point of attack connected with blockchain.**

2.	**Iuon-Chang Lin**	**2017**	**Not mention**	**Covered**	**Concerns about safety and a variety of other problems are addressed.**
3.	**Zibin Zheng**	**2016**	**Moderate**	**Not Covered**	**Presented a review on the blockchain's taxonomy, as well as the related consensus protocol and application field, and discussed it.**
4.	**Bayu Adhi Tama**	**2017**	**General Study**	**Not Covered**	**An examination of the current condition of the blockchain application field is carried out.**
5.	**Bhabendu Kumar Mohanta**	**2018**	**Extensive Most area**	**Covered**	**conducting a review of five distinct research databases, locating the use of blockchain technology, and providing a categorical explanation of each article. Additionally, the possible applications of blockchain technology should be identified, and the associated security concerns should be mentioned.**

Blockchain Design

The underlying distributed ledger technology that facilitates bitcoin transactions is known as blockchain. This category of database is characterised by having the characteristics of a public distributed database that also features an encrypted ledger as an integral element of its operational capabilities. Blockchain technology is a decentralised and distributed ledger that can be viewed by anybody who has access to the internet. Using this technology, transactions may be recorded and validated to ensure that they are legitimate. Blockchain does not belong to anybody and can be viewed by everyone. This is in contrast to traditional databases, which are usually controlled by centralised entities such as banks and governments. Because of the fact that the entire network is keeping an eye out for it, it is extremely difficult, if not impossible, to trick the system with a bogus document, transaction, or other piece of information because the network as a whole is watching out for it. Blockchain refers to a distributed ledger

that maintains information in an immutable manner in a network that is shared by numerous nodes. A blockchain is shared by multiple nodes. It is not just about the decentralisation of information, but also about the way that information is disseminated around the world.

Every node in the network is able to store its own local copy of the Blockchain system, which is then routinely updated to ensure that all copies are consistent with one another and with the original. This ensures that transactions can be verified and recorded accurately.

Blockchain is a distributed computing and information sharing platform that enables a number of nodes to adopt a decision-making process even when they do not trust each other. This is made possible by the fact that blockchain uses cryptography to ensure that nodes cannot impersonate each other. Satoshi Nakamoto, the inventor of Bitcoin, is credited with developing blockchain. The fact that centralised systems only have a single potential failure point is the primary drawback that is linked with using such systems. In a decentralised system, instead of having a single vulnerable point that is centralised, there are several coordinate points that are dispersed across the system. Because of this, there is no longer any chance that the entire system will become inoperable. When carrying out a task in a setting that is dispersed among several nodes, every single one of those nodes makes a contribution to the overall outcome of the task.

The fundamental makeup of Blockchain is depicted pictorially in Figure 1, which may be found here. Every single user was given a graphical representation in the form of a node that was connected to various other nodes in a decentralised manner. Every node in the network was responsible for saving their own copy of the Blockchain list, which was then kept in a state of perpetually accurate and up-to-date status. A node is capable of doing a variety of tasks, such as mining, verifying transactions, and initiating transactions, amongst other things. Mining is an activity that generates new coins for the blockchain.

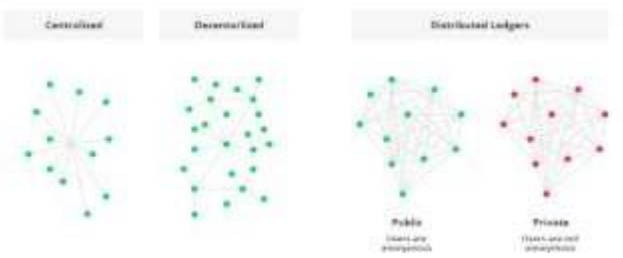


Fig 1: Block chain Architecture

Blockchain Technology Structure

When talking about Blockchain, the term "block" refers to a collection of transactions that are thought to be legitimate. A distributed ledger is a sort of ledger that allows any node in the system to begin a transaction and broadcast it to all of the other nodes in the network. This type of ledger is known as a blockchain. Blockchain technology is utilised within cryptocurrencies such as bitcoin. The subsequent phase, which takes place after a transaction has been validated by the nodes of the network by being compared to previously validated transactions, is to add the newly validated transaction to the Blockchain that is already operational. This phase takes place after a transaction has been validated by the nodes of the network by being compared to previously validated transactions. The entire number of transactions that took place during that time period is tallied as a component of the block, and the block is then kept as an essential component of the Blockchain when the counting process is complete. The

upper bound suggestion made by Satoshi Nakamoto in 2010 states that Bitcoin "A block may consist more than 500 transactions on average, and the average size of a block is roughly 1 MB." At some point, it is feasible that it will reach 8 MB, and there is even a chance that it could go higher (as of March 2018). The use of blocks that are noticeably larger in size can make the processing of a substantial number of transactions substantially simpler. The specifics of the Blockchain system are broken down and elucidated in each individual section of the graphic that is provided below.

• There are two separate facets to consider: In addition to a transaction list, the header of each block will have its own unique identifier. The information pertaining to the following categories and subcategories may be found inside the header of a block:

• Previous Block hash: The hash of the block that was there before a later block is something that is inherited by the block that comes after it.

• It is not possible to alter the Blockchain in any way since the system utilizes the hashes of previous blocks to build the hashes of new blocks. This makes it immune to manipulation.

• The following are some mining statistics that were used in the process of constructing the block: In order to guarantee that the Blockchain cannot be manipulated in any way, Bitcoin Mining necessitates the use of a method that is adequately complicated.

Types of Blockchain

There are presently three unique varieties of blockchains, which are known as public blockchains, private blockchains, and consortium blockchains.

A public blockchain is a type of blockchain in which the ledgers are viewable by anyone who has access to the internet. Additionally, anybody may verify and add a block of transactions to a public blockchain.

In a private blockchain, only a restricted number of people inside an organization are allowed to verify and add new transaction blocks, whereas in a public blockchain, anybody who has access to the internet is able to see the contents of the ledger.

Although the ledger may be open to the public or confined to a specific group, under this approach, only a collection of organizations (like banks) is able to check and add transactions.

Application of Blockchain Technology

The concept that would later become known as blockchain technology originated with the digital currency known as bitcoin; but, since its inception, this concept has been used to a wide range of diverse areas. The applications of Blockchain that are explained in the following paragraph are summarized here. These applications include those in the fields of finance, healthcare, the Internet of Things, legal perspectives, government, power grids, transportation systems, commercial world, cloud computing, reputation, electronic business, and supply chains.

- Healthcare
- Financial
- Internet of things

- Government
- Cloud computing

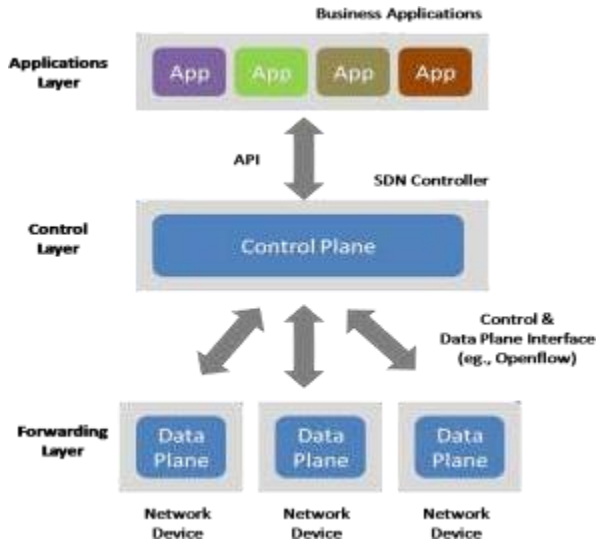
Software Design Network

Software Defined Networking is the name of the technology that stands in stark contrast to blockchain technology (SDN). In a software entity known as the SDN controller, network management and configuration tasks are consolidated in a system that employs software-defined networking (SDN). The recording of transactions is done by blockchain technology using decentralised ledgers. The architecture of software-defined networking (SDN), which divides the data plane from the control plane, has resolved a number of security problems that are common in conventional networks while simultaneously opening up new entry points for attacks. In the event that certain network services are dispersed in a manner that is comparable to the execution of the technology that underpins Blockchain, there is a good chance that the security concerns connected to the SDN architecture will increase.

This is due to the fact that the occurrence of this event is quite likely. The term "Software-Defined Networking," or SDN for short, refers to a technology that is not all that old but was just recently embraced in order to expedite and simplify the process of setting up and administering networks. This technology is not all that old but was just recently embraced in order to simplify the process of setting up and administering networks. This technology has been used very recently in order to streamline the process of establishing new networks and managing existing ones. Despite its relatively young age, this innovation has proven to be rather useful. This innovation is starting to garner substantial interest not just from the commercial sector but also from the academic community as a whole. It is a relatively new method of building networks that support a more robust environment by bringing reliability and security to the forefront of the process to prevent, detect, report, isolate, minimise, and eventually mitigate the harmful effects of the majority of network breaches. This can be accomplished by bringing reliability and security to the forefront of the process. Putting trustworthiness and safety at the forefront of the process is one way to achieve this goal. Putting reliability and precautionary measures at the centre of the process is one method to work toward the achievement of this objective. One approach to working toward the accomplishment of this goal is to make the maximisation of dependability and the utilisation of safety precautions the primary focus of the process. The fundamental idea that has fueled the innovation processes in the SDN technology is the centralization of the control plane, which in traditional networks is distributed along with the functionality of the data plane inside the routers and switches. This idea is at the heart of the software-defined networking (SDN) technology. This concept has been the impetus for the creation of software-defined networking technology (SDN). This idea is crucial to the software-defined networking (SDN) technology that is undergoing development at the moment. The technology known as software-defined networking (SDN) is being driven forward by this concept, which serves as the engine. The software-defined network (SDN) is acknowledged to contain the control plane as an essential component (network intelligence).

This is typically separate from the portion of the network that is in charge of the transmission and transmission of network traffic, i.e., the control plane is typically logically centralised in a software entity known as an SDN controller. This section of the network is responsible for the transmission and transmission of network traffic. This separation ensures that the component of the network that is in charge of deciding how to route network packets will remain untouched by any issues that may arise in other portions of the network, regardless of the nature of those issues. If a network administrator has access to an SDN controller, it is much simpler for them to programme and

configure all of the parts of the network directly from a single control point than it is for them to have to physically access each individual network device. This makes it much more efficient for the administrator to manage the network. This is due to the fact that the SDN controller allows for the programming and configuration of any and all components of the network directly.



Security and privacy in Blockchain and Software Design Network

The blockchain operates much like a public ledger, but it must guarantee a variety of distinct elements, including the following:

Software Design Network Architecture

- Protocols for Commitment: Ensure that each and every genuine transaction that is sent in by clients is committed and added to the Blockchain within a specific length of time. This might vary depending on the protocol.

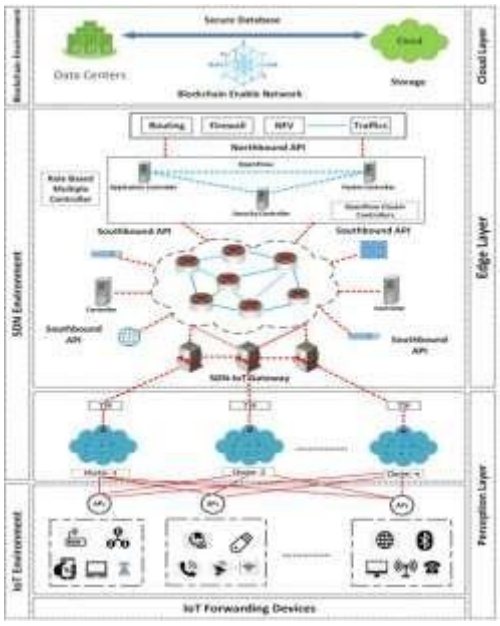
- There is widespread consensus that you should check to see that the local copies contain correct and up-to-date information.

- It is imperative that the data remain unchangeable at all times from a safety perspective.

- There is a chance that some of the nodes may act maliciously or that they will be hacked. Both of these outcomes are probable.

- The fact that the data and transactions are owned by several nodes serves to protect both their privacy and their legitimacy.

- As a result, it is necessary to safeguard both the legitimacy and the right to personal privacy. The concept of blockchain, which was first introduced with the cryptocurrency bitcoin, has evolved into an appealing technology for peer-to-peer transactions, the integrity of data, and transparent storage in a decentralized environment.



Many different applications of the Blockchain technology leave it vulnerable to many different threats and assaults. Some of these hazards and attacks include double spending, privacy leakage, private key security, mining attack, and balancing attack. In this section, a brief discussion is had on a number of different academic projects that have already been finished. The issue of safeguarding and maintaining users' privacy inside the Blockchain has attracted the attention of a number of researchers, who have focused their attention on the topic. When it comes to the process of hashing transactions on the Blockchain, one of the most essential issues is that of cryptographic primitives, as well as privacy and anonymity. In the course of the mining process, a broad range of cryptographic techniques are utilized, and the consensus algorithms of Bitcoin and Ethereum are contrasted and proposed. The benefits of using Open Distributed Ledgers (ODL) for the authentication of users while providing Trust Management security.

The Blockchain technology's transaction authentication function, which removes risks and ensures data integrity, has the potential to make data integrity a reality. Blockchain technology includes a function known as transaction authentication. The aforementioned publication presented not only the idea but also the procedure for verifying the quality of a selected verifier.

bitcoin exchange, in addition to the building of the first concrete method to implement a specified proof-of-asset verification for bitcoin exchange using elliptic curve cryptography. Both of these accomplishments were made by the same team. The same team is responsible for both of these milestones, which they have achieved. A method that could be utilized to make the system more secure is the incorporation of a framework that is based on public key infrastructure with the Cecoin distributed PKI scheme. Implementing blockchain technology requires careful consideration of several factors, not the least of which is the protection of the online identities and privacy of blockchain users.

The purpose of the research that was described in was to develop a model for the effective cooperative uploading of material in cellular environments based on D2D proximity communication. An innovative trust-based strategy was presented as the solution to the problem. A number of attacks, such as code-based, double-spend,

transaction-dust, and double-spend assaults, are capable of being launched against certain programmes. In light of these attacks, it is imperative that appropriate measures be taken. The resiliency of the Bitcoin ecosystem, the obviousness of its application of blockchain technology, the widespread distribution of transaction blocks, and the following verification of those blocks. The demonstrated a system that is composed of conventional Proof-of-Work-based deployments in addition to Proof-of-Work Blockchain variants. These variations are built with different characteristics, and then the trade-offs between their performance and security measures are objectively analyzed. In this day and age, when our capabilities to acquire and analyses the data of individuals are always improving, it is becoming increasingly necessary to have ownership of the data that is generated by the network. In other words, it is becoming increasingly important to have control over the data.

The Blockchain technology may be able to provide users with more privacy by suggesting a fraud protection system for odometers. This is a solution that has been devised in response to the problems that have been outlined. Because the application records the miles driven by vehicles as well as their GPS coordinates and saves this information in an encrypted format on the blockchain, it is far more difficult for false odometer readings to take place. When using some programmes in which the network architecture interacts with the internet, you will be required to implement safety precautions in order to guard yourself from dangers posed by the internet, such as ransomware. In order to prevent the possibility of ransomware attacks, the application infrastructure has to be safeguarded against unauthorized access from the outside. The Byzantine-fault tolerant ordering service for the Hyperledger Fabric Blockchain platform that uses the BFT-Smart replication library is an additional kind of attack that seeks to tackle the privacy and security problem. This form of attack makes use of the BFT-Smart replication library. The execution that is replicable on Ethereum's private chain and a description of the conditions under which Blockchain solutions are unable to reach agreement.

The study that was given featured both an overview and an examination of the security features that Bitcoin and the Blockchain, the technology that supports Bitcoin, provide for users. These safeguards were effective in preventing the system from being compromised by the attacks and threats that had been recorded in the past.

The research presented in this paper analyses and evaluates a variety of preventative actions that may be taken in the event that an assault is launched against the system. Some of these preventative measures have already been included into the system. Using the characteristics of the blockchain, a mechanism has been developed that allows for the secure utilization of drones as on-demand nodes for the interoperability of services supplied by a number of different suppliers. If the issues surrounding the protection of personal privacy are not effectively managed, it may result in economic and reputational losses, inhibit the invention of network and e-commerce technologies, and lead to a variety of other effects. These issues have gradually prompted widespread concern in society.

Conclusion

Because it decentralises data and eliminates the need for a trusted third party in a peer-to-peer (P2P) network, blockchain technology is the antithesis of the concept known as software-defined networking (SDN). To phrase it another way, the SDN model is dependent on a reliable third party. The ability of a blockchain to conduct transactions in a public, private, or in a consortium setting is what decides whether or not it is a public, private, or consortium blockchain. All of the nodes in a public blockchain are included in the mechanism that achieves a consensus, and all of the nodes have access to the data that is associated with the transactions. In private and

consortium blockchains, transaction access can be given or cancelled based on a decision made by a centralised entity. Public blockchains, on the other hand, do not have this restriction. In addition, the consensus process is only used by a restricted number of nodes that have been validated in advance.

In this post, we will examine previous initiatives that have merged SDN technology with Blockchain technology in order to establish effective cybersecurity solutions for securing SDN architecture from attacks. This will be done in order to establish effective solutions for securing SDN architecture from potential threats. The purpose of this article is to offer an overview of these activities. Even though research initiatives have made significant progress toward the goal of protecting software-defined networks (SDN), an intrusion detection and threat mitigation system that is capable of protecting the control and data planes in addition to the communication channel has not yet been developed. This is despite the fact that these initiatives have made significant headway toward the goal. The paper also presented a strategic vision for making use of Blockchain technology and making the most of the characteristics it offers in order to both guarantee the safety of SDN and open the door to an SDN architecture that is more scalable and effective. This came about as a direct result of the previous point. This was done in order to successfully accomplish both of these objectives at the same time.

References:

[1] A.Z. Broder, M. Mitzenmacher, Network applications of Bloom filters: A survey, Internet Math. 1 (4) (2003).
[2] B.H. Bloom, Space/time trade-offs in hash coding with allowable errors, Commun. ACM 13 (7) (1970) 422–426.
[3] H. Cai, P. Ge, J. Wang, Applications of Bloom filters in peer-to-peer systems: Issues and questions, in: NAS'08: Proceedings of the 2008 International Conference on Networking, Architecture, and Storage, Washington, DC, USA, 2008, pp. 97–103.
[4] P. Hebden, A. Pearce, Data-centric routing using Bloom filters in wireless sensor networks, in: M. Palaniswami (Ed.), Fourth International Conference on Intelligent Sensing and Information Processing (ICISIP-06), IEEE Press, Bangalore, India, 2006, pp. 72–78.
[5] T. Wolf, Data path credentials for high-performance capabilitiesbased networks, in: ANCS'08: Proceedings of the 4th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, ACM, New York, NY, USA, 2008, pp. 129–130.
[6] F. Ye, H. Luo, S. Lu, L. Zhang, S. Member, Statistical en-route filtering of injected false data in sensor networks, in: INFOCOM, 2004, pp.839–850.
[7] S. Ratnasamy, A. Ermolinskiy, S. Shenker, Revisiting IP multicast, in: Proceedings of ACM SIGCOMM'06, Pisa, Italy, 2006.
[8] P. Jokela, A. Zahemszky, C. Esteve, S. Arianfar, P. Nikander, LIPSIN:line speed publish/subscribe inter-networking, in: Proceedings of ACM SIGCOMM'09, Barcelona, Spain, 2009.
[9] S. Dharmapurikar, P. Krishnamurthy, and D. E. Taylor. Longest prefix matching using Bloom filters. In Proc. ACM SIGCOMM, Karlsruhe, Germany, Aug. 2003.
[10] M. Dietzfelbinger and C. Weidling. Balanced allocation and dictionaries with tightly packed constant size bins. Theoretical Computer Science, 380(1):47–68, 2007.
[11] B. Fan, D. G. Andersen, and M. Kaminsky. MemC3: Compact and concurrent memcache with dumber caching and smarter hashing. In Proc. 10th USENIX NSDI, Lombard, IL, Apr. 2013.
[12] L. Fan, P. Cao, J. Almeida, and A. Z. Broder. Summary cache:A scalable wide-area Web cache sharing protocol. In Proc. ACM SIGCOMM, Vancouver, BC, Canada, Sept. 1998.

[13] N. Fountoulakis, M. Khosla, and K. Panagiotou. The multipleorientability thresholds for random hypergraphs. In Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, pages 1222–1236. SIAM, 2011.
[14] N. Hua, H. C. Zhao, B. Lin, and J. J. Xu. Rank-Indexed Hashing: A Compact Construction of Bloom Filters and Variants. In Proc. of IEEE Int'l Conf. on Network Protocols (ICNP) 2008, Orlando, Florida, USA, Oct. 2008.