International Journal of Electrical, Electronics and Computers
Vol-6, Issue-5 | Sep-Oct, 2021
Available: https://aipublications.com/ijeec/
Peer-Reviewed Journal

A Novel Blockchain based Software Defined Network (SDN) Architecture to Curb the Impact of DoS/DDoS

Subhasis Sanyal, Mohit Kumar Barai, Anil Goplani

Samsung Research Institute, Noida, India.

Received: 27 Jul 2021; Accepted: 24 Sep 2021; Date of Publication: 02 Oct 2021

Abstract— *The proliferation of virtualization or containerization has created a new state of the art in the networking domain; Software Defined Networking (SDN). In the prior state of the art, networking was performed through two abstractions, a "Data plane" and a "Control plane." Whereas in SDN, it's done via a new centralized "Network OS" and a "Virtualization Layer." The "Network OS" runs on servers, observing and controlling the data plane of the "Virtualization Layer." Even though this architecture has given flexibility and agility to new network development and management, but it has created various security vulnerabilities like confidentiality, integrity, availability, etc. Here in this paper, a novel blockchain-based architecture has been proposed to unravel a particular issue, denial of services (DoS). In the proposed state of the art, a novel layered architecture has been considered. From the top, the control plane has been decomposed into a decentralized blockchain layer. A fog layer follows this. Blockchain-based multiple fog nodes or fog servers will be connected to numerous blockchain light nodes inside the fog layer. The user plane will be directly related to the fog layer. Also, here a particular type of intelligent node has been introduced. The proposed state-of-the-art shows more willingness and adaptability to surpass the challenges of vulnerabilities due to DoS and DDoS while maintaining scalability*.

Keywords— ***Blockchain, Chaos Theory, Control Plane, Fog Server, User Plane, Software-Defined network.***

I. INTRODUCTION

Lack of scalability, adaptability, flexibility, and speed in a traditional network, has given birth to "Teleco Cloud" [3,4]. The component of Teleco Cloud, Network Function Virtualization (NFV), and SDN (Software Defined Network) is the convergence between cloud computing and telecom networking, supporting real-time on-demand capacity and reachability with minimum latency. Here our topic of discussion is SDN and its security concern. Software-defined networks (SDNs) decouples the data plane from their control management plane. It replaces the conventional TCP/IP architecture [1,2]. The control plane and data plane were coupled as a unified body in traditional networking architecture. In a Software-defined network, the control plane becomes a central entity or brain to govern the user plane. With this convention, the OPEX and CAPEX of network management can be reduced drastically. Gartner's research indicates that a move to SDN-enabled switches replaces expensive core switching platforms and can deliver capital savings of between 30% and 70% (CAPEX), with OPEX savings of over 30% [13]. The cause of OPEX saving is the reduction of manual work on individual servers and switches. With virtualization/containerization, many functions can be rolled up and managed at a time. A small group of network engineers can manage more setup, deployments, and troubleshooting. CAPEX reduction because virtualization of network resources allows less use of high-end equipment. It will enable organizations to get more out of less and scale at a less incremental value. It can reduce redundant capacity needs and costs.

Many multi-controller or uni-controller SDN had been proposed with vertical and horizontal type communications to manage and control the massive or large-scale networks. In vertical communication, OpenFlow [5], like protocol on top of the Transmission Control Protocol (TCP) and combination of Transport Layer

Security (TLS) protocol, manages the southbound interface between the Controller and the forwarding devices by telling the switches where to send data flows. The northbound interface helps to manage the communication between the Controller and the applications. In horizontal communication, multi-controller environment controllers exchange information about network topology between them by their east-west interfaces. It is paramount for the Controller to maintain a global network view. SDN has one layered routing and one layer of centralized management, so the primary emphasis has to be given to security [6,7,8,9,10,11]. A compromised controller can send fraudulent flow information to switches in the data plane or other controllers in multi-controller architecture, leading to various Denial of Services (DoS) and malfunction. The aggregation of the entire network management and configuration in a centralized SDN controller can be considered a single point of failure in the case of DoS.

The proposed state of art advocates a decentralized blockchain-based controller plane with full nodes and a Fog layered user plane with light blockchain nodes to impede the above effect. Managing a decentralized database by multiple participants with distributed consensus is called Distributed Ledger Technology (DLT). Blockchain is a DLT in which transactions are recorded with an immutable cryptographic signature called a hash. A node (block) contains data, a hash value, and the previous block's hash value in the blockchain. A node in a blockchain has three particular basic tasks like storing and saving a block's transaction history, validating a new block, and updating other nodes in the blockchain to ensure all nodes on the blockchain have the latest information. It is easy to detect changes when the hash is utilized—the main reason for ever rocketing interest in blockchain is its applicability in virtual infrastructure. Blockchain solves the problem of trust and provides transparency, immutability, traceability, and security. It is a decentralized P2P-based transparent network where complete control is given to the user without the intervention of a middleman. Due to its decentralized nature, the scope of scalability is very massive. But the question is can it subdue the problem of DoS? It has been shown that a '51% attack' in cryptocurrency is the most severe DoS attack. In a '51% attack,' one miner or mining group gains enough hash power to take control of 51% or more of a blockchain network and double-spend the cryptocurrency involved. But the chances are significantly less due to complex mathematical hashes and computing power limitations a miner has to go with [17]. We can consider the same impact as 'A grey swan' impact in our blockchain-based SDN, where the event is known and potentially extraordinarily significant but considered not very likely to happen. So, we can say utilization of blockchain-based system decentralized not only the Control Plane but also User plane somewhat can suppress the massive impact of DoS. But still, the effect of DDoS we need to look for.

Fog computing is an extended version of cloud computing. Fog computing services are near to the end devices. Due to proximity to the end devices, this computing paradigm is a significant advantage over other traditional computing models [14]. The significant Fog characteristics are its dense distribution and its mobility support. Services are hosted by the network edge or even end devices such as set-top-boxes or access points. By doing it, Fog reduces service latency and improves QoS, resulting in a superior user experience. Fog Computing supports emerging IoT applications that demand real-time/predictable latency (industrial automation, transportation, networks of sensors, and actuators). Thanks to its wide geographical distribution, the Fog paradigm is aptly positioned for big real-time data and real-time analytics. Fog supports closely distributed data collection points, adding a fourth axis to the often-mentioned Big Data dimensions (volume, variety, and velocity). The drawbacks of cloud computing, like the risk of data confidentiality, level of security, and data encryption, have been curbed by fog computing to more precisely secure user data [12]. Fog applications can keep detailed personal data at the edge, transferring only aggregated or properly anonymized data to the cloud.

Many existing studies highlight security and other issues with SDN. We have pin down a specific scenario in which the SDN architecture becomes vulnerable to attackers. These vulnerabilities allow attackers to enforce a distributed denial of service (DDoS) attack on the network. The DDoS attack can be performed by frequently sending unique packets requests to the Controller. For this research study, we are trying to curb DDoS or DoS. Cisco has forecasted, the total number of DDoS attacks will increase doubly from 7.9 million in 2018 to something over 15 million by 2023. [16]. A10 State of DDoS Weapons Report for H2 2020 has suggested an expansion of over 12% in the number of potential DDoS weapons. A total of nearly 12.5 million weapons has been detected. It can lead to severe real-time network traffic management issues [15].

We propose a distributed architecture with a Fog layer between SDN's infrastructure and control layers to address the earlier issue. It has distributed Fog nodes or servers, which are full blockchain nodes, gradually increasing based on transaction demand. An algorithm can be used for dynamic node/server allocation by which server load-balancing can be maintained. These nodes are connected to multiple light node blockchain nodes. These nodes hold transaction information state request/reply from

individual switches/firewalls. Each node of the Fog layer has been connected to the multiple controller nodes. Also, for the control layer, a single master controller and multiple redundant controllers have been considered. Here the controllers are members of the blockchain. The master controller creates blocks, and redundant nodes in blockchain monitor its behavior. It helps secure inter-controller communication.

Our objective is to detect DoS or DDoS in the system (SDN) and minimize its impact. We have categorized two types of user transaction blocks, one who's are authenticated and the other who has the potential to become malicious, the reason for the DoS attack. We have tried to apply the "Chaotic Dynamical System" phenomenon to detect any potential DoS-related network issues. Because chaos is more about nonlinearity (i.e., A influences B, which in turn influences A, but all of this occurs in continuous time), the outcome of the Chaotic system is not random. The wild deviations in output can be predicted deterministically from even small changes in initial conditions. So, there is "order" (as opposed to randomness and unpredictability) in chaos. We have tried to implement this phenomenon during block creation and transactions during north-southbound or east-westbound traffic control and management between Control Plane and Data Plane.

After that, we have attempted to utilize 'Bayesian Nash Equilibrium' between authenticated and malicious block transactions. Where chosen strategy of an established transaction block we call it as 'Random blocks' and will provide the best possible results out of all the possible approaches, regardless of the strategy that the malicious transaction block or uses. For vicious block, we have chosen a name called 'Superblock.' At the same time, the system will generate blocking control over negative transaction blocks. Our proposed solution considers each block as a self-sufficient and intelligent block that can make transaction decisions. This type of block has been tuned with a distributed DNN model. All blocks are self-replica when it comes to decision-making, even though they may have a different state at a specific time. Our proposed hypothesis can help the system prevent the DoS attack and expedite scheduling and load balancing among various nodes and increase the overall efficiency of the SDN network. Also, the use of blockchain with our proposed method gives us two layers of securities. One from use of blockchain itself as with ever-growing nodes in Blockchain-based system decreases the chances of '51% attack' as the cost of penetrating network is very high for any miner. Also use of Intelligent autonomous distributed blockchain nodes gives another edge of various kinds of DoS attacks. The use of the proposed architecture decreases the latency as blockchain nodes in the data plane in case any suspicious action can take its own decision without further forwarding the request to Controller.

II. THE OBJECTIVE OF STUDY, RELATED WORK, AND NOVELTY

Switch from traditional networks to Software-Defined Networks (SDN) is invigorated due to more flexibility, efficiency, and cost-effectiveness. But most of the SDN development is within the purview of features, not security; these SDNs are vulnerable to numerous attack vectors; also centralized nature of SDN appends more security concerns. In traditional networks, hosts or servers on the network would primarily be at risk from attacks, but now with SDN, new APIs and vulnerabilities are exhibited for the network itself. Once a single reprobate element like a switch or firewall, injected by a hacker and is accepted by an SDN, it can disrupt communications on the network in various ways. Denial of Services (DoS) is one of them. Therefore, any holistic security system is needed to counter these menaces to Software-Defined Networks. At the same time, the impact of SDN's performance should maintain a standard; also, it will be able to generate warning signs and a forensically auditable log about the states on the network. Many researchers have propounded several solutions to restrain the security issue like DoS. Blockchain is one of them. The use of Blockchain in SDN captures a forensically auditable and unchangeable log of anything that happens on the SDN, which can further be utilized to reject any alteration from a rouge peer. In their research paper, Blockchain-based Controller Against False Flow Rule Injection in S.D.N., Boukria, et al. [23] has provided a blockchain-based method to enhance the SDN controller's security. Their objective was based on attack detection and prevention. In another research paper, Towards Blockchain-Based Software-Defined Networking: Security Challenges and Solutions, Wenjuan et al. [24] have provided a solution for security concerns by decentralizing the control plane using blockchain. In their research paper, Yazdinejad et al. [25] has proposed a secure and energy-efficient blockchain-enabled architecture of SDN controllers for IoT networks using a cluster structure with a new routing protocol. They have used public and private blockchains for peer-to-peer (P2P) communication between IoT devices and SDN controllers. In another research work, Block Flow: A Decentralized SDN Controller Using Block-chain, Krishnamohan et al. [26] had proposed a holistic Blockchain-based control plane that will curb the Denial-of-Service attacks. In their research paper, Tselios et al. [27] describes the Blockchain paradigm's design principles and advocated the reasons that render blockchain as a significant

security factor for solutions when SDN and IoT are integrated.

The idea of decentralizing the control unit seems ubiquitous in various research papers to tackle the DoS issue. By our research work, we also strongly support that. However, the decentralized nature of blockchain drastically limits its performance (e.g., throughput and latency) [29]. For example, well-known cryptocurrency Bitcoin can only achieve a low throughput of 7 transactions per second (TPS), and it takes around 10 minutes for a transaction to get confirmed [28]. But to deploy the concept of Blockchain-based control plane SDN in 5G NR where URLCC (Ultra Reliability Low Latency Communication) and eMBB (Enhance Mobile Broadband) are the prime attributes, it may hinder the Quality of Services (QoS) that it promises to deliver. Our proposed solution to mitigate the before mentioned QoS advocates a Blockchain-based SDN system where both control and user plane can be structured with the help of intelligent blockchain nodes. Each can make its own decisions about flow control in the network. If an intelligent node in the user plane detects the flow request is malicious, it can restrict it with further forwarding to control plane nodes. This sort of communication will automatically maintain the reduced latency factor. Also, in our proposed architecture, the user plane nodes are driven by light blockchain nodes. Light nodes are those entities that prefer to store only a subset of the blocks connected to a Full node. In our case, the full node is a Fog server. This kind of architecture will create a performance enhancement from all proposed prior art in this field.

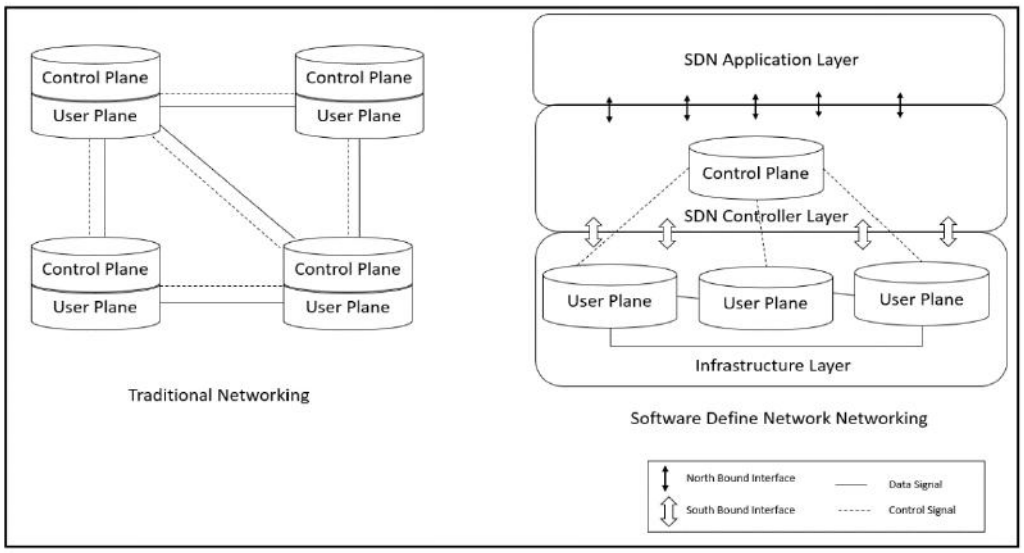

Fig 1. Difference between Traditional and SDN Network

III. BACKGROUND

A. SDN (SOFTWARE-DEFINED NETWORK):

We are living in a world where open-source platform thrives innovation. Open source enriches ingenuity; a programmer or community of programmers can use pre-existing code to enhance the software and even develop their inventions. All prior arts related to traditional networking were predominately based on proprietary Network switches in data centers. The maintenance and management costs were huge, and the innovation in networking was slow. Today, data centers are exploding. The networks in these data centers cannot deal with changing workflows like a cloud where tenants come and go, where the network is bursty, and it costs tons of money to keep hardware that would otherwise be idle powered up and cool. As a result, a researcher in networking was dealing with all of the issues related to giant cloud data centers. To restrain this impact researcher has developed a concept of virtualization and containerization, and the open-source paradigm has given an ultra edge to this state of arts. SDN or Software define network is a state of the art where decoupling software from hardware has been done by taking aide from virtualization and open-source platform. Routers/Switches are programmable components on opensource. Any experience coder can deploy their protocol to the router/switch with the help of OpenFlow 2.0. Also, it's possible to deploy the traditional age-old protocols like SNMP, OSPF, UPnP, NAT, NTP, etc., on the routers & switches. The software can define the network, i.e., protocols to be handled in the switches and treat the packets in the network device. But to support this infrastructure, there was a need to separate the Intelligence and Datapath. The Control Plane, which consisted of all the intelligence of routing protocols, configuration, etc., is moved out of the box and kept centrally, which can control many network

devices at a time. One analogy can be given here: our brain is centralized, and we have so many parts of our body acting on the brain's commands. So, SDN is a new paradigm in networking that allows virtualizing the network.

OpenFlow allows the control plane to be co-located on a compute node in a data center and an agent running on the switch. In simple terms, the compute node half of OpenFlow can read statistics from the switch and change the forwarding plane in response by sending commands to the OpenFlow agent on the switch.

B. PROBLEM OF CENTRALIZED CONTROL PLANE AND DOS/DDOS ATTACKS:

Various types of network topologies are available here in the context of SDN. We will describe a few of them relevant to our research work. A system whose components are located on different networks, and to coordinate, they pass messages among them known as a Distributed System.

A Decentralized network architecture distributes its workloads among several machines instead of a single central server unit. In contrast, a Centralized network architecture is built around a single service point that handles significant processing. The Control plane controller or the brain part of SDN is a dynamic manager who single-handedly commands and manages the traffic request once it receives it from the data plane or user plane. The Controller takes all the decisions by entrusting the only implementation to the subordinates. Few factors govern the brain part like Uniformity of action, Facilitating Integration, Handling Emergencies. One of the significant issues with a centralized controlling system is that it can't scale up vertically once a specific limit has been reached – After that limit, even if we increase the hardware and software capabilities of the central server node, the performance will not increase ultimately leading to a cost/benefit ratio < 1.

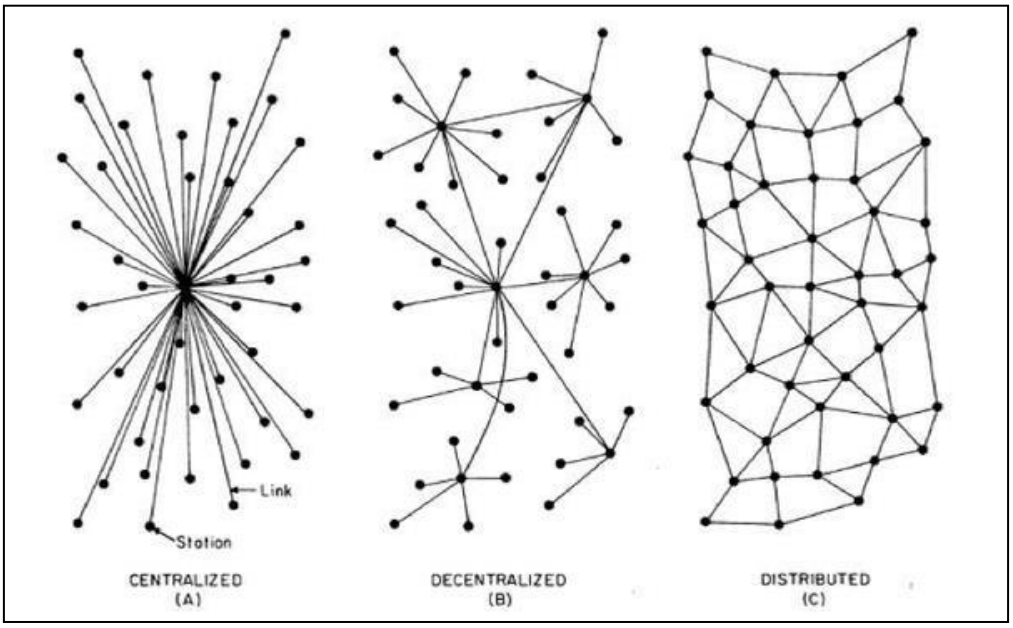

Fig 2. System topology of centralized, decentralized, and distributed system

Another major problem is when the traffic spikes as the controlling server have a finite open port. It can listen to the clients, leading to a Denial-of-Service attack or Distributed Denial-of-Service attack—flooding a network with ineffectual data so that authentic traffic cannot get through. Various kinds of DoS attacks are available. An imposter user can remotely overload a system's CPU so that valid requests cannot be processed. One typical example is triggering a rapid series of false login attempts that lockout accounts from logging in. The most common type of DoS attacks are,

i) ICMP flood – It leverages misconfigured network devices. An intruder sends spoofed packets that ping every other host on the targeted network instead of just one specific host. The network was eventually triggered to amplify the traffic. This attack is also known as the 'smurf attack' or 'ping of death.'

ii) SYN flood – An intruder sends a request to connect to a server host, but it never completes the handshake. And it continues until all open ports are entirely saturated with requests, and for this, suddenly, no ports become available for legitimate users to connect with.

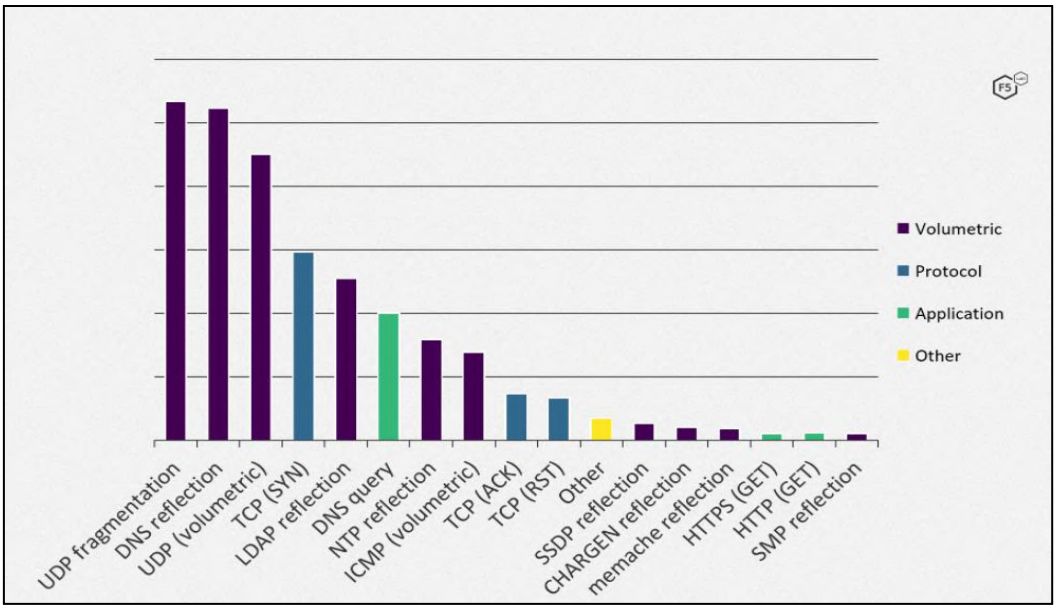

Fig 3. Various types of DoS or DDoS attacks in 2020 January to 2021 March [30]

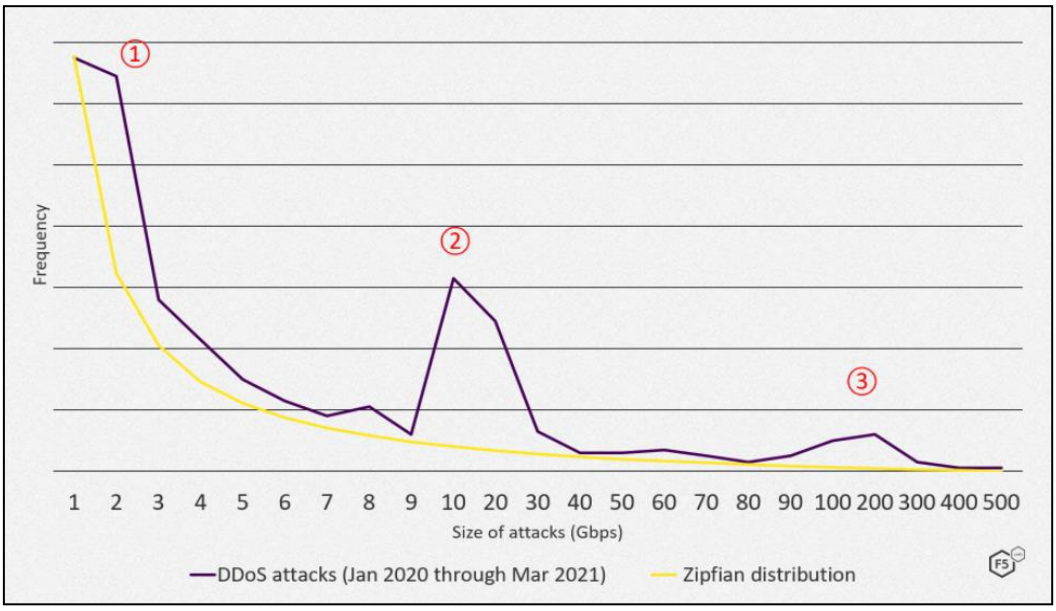

Fig 4. Distribution of DDoS attacks [30]

One of the most vicious types of DoS attacks is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when collective systems orchestrate a synchronized DoS attack to a single target. Here, instead of being attacked from one place, the target is attacked from many places at once. The distribution of hosts in a DDoS provides the attacker immense advantages. Also, they are hard to detect due to the random distribution of the attacking system. The impact of the DoS attack is enormous. Any SDN model can be hugely targeted by DoS and DDoS, leading to complete system failure. So, to restrain the effects of DoS or DDoS, decentralization of Controller is required; else it will fail to provide promised QoS. Below are some data supplied by the F5 lab, Application threat, and intelligence [30].

In Figure 4, Zipfian distribution is the probability of occurrence that follows Zipf's law, which relates rank order and frequency of occurrence.

C. IMPORTANCE OF BLOCKCHAIN:

Invented by Satoshi Nakamoto in 2008, blockchain was a revolution in the digital world. It became a pioneer of a decentralized network to store data. The entire process has three ingredients: Blocks, Nodes, and Miners. A block

accommodates the data records. Each block contains a unique randomly generated number—a reference to the previous block. Miners are the persons who create new blocks. They use special software to do so. They have to solve a very complex math problem to create a block. For a new transaction to be updated, they have to be approved by the network of nodes. Due to decentralization, people can check each transaction. The authenticity of blockchain is secured by digital signature. Blockchain is tamper-proof and cannot be changed for its encryption and digital signatures. All the network participants in blockchain reach an agreement that is familiar as consensus. For all the network participants, a common history is obtainable as the data in the blockchain is recorded digitally, reducing the probability of fraudulent activity or duplication of transactions without the intervention of a third party. The potentiality of blockchain is immense. According to Gartner, an annual business value of more than US $3 trillion by 2030 will be generated by blockchain. It's also possible to imagine that 10% to 20% of global economic infrastructure will be running on blockchain-based systems by that same year [31].

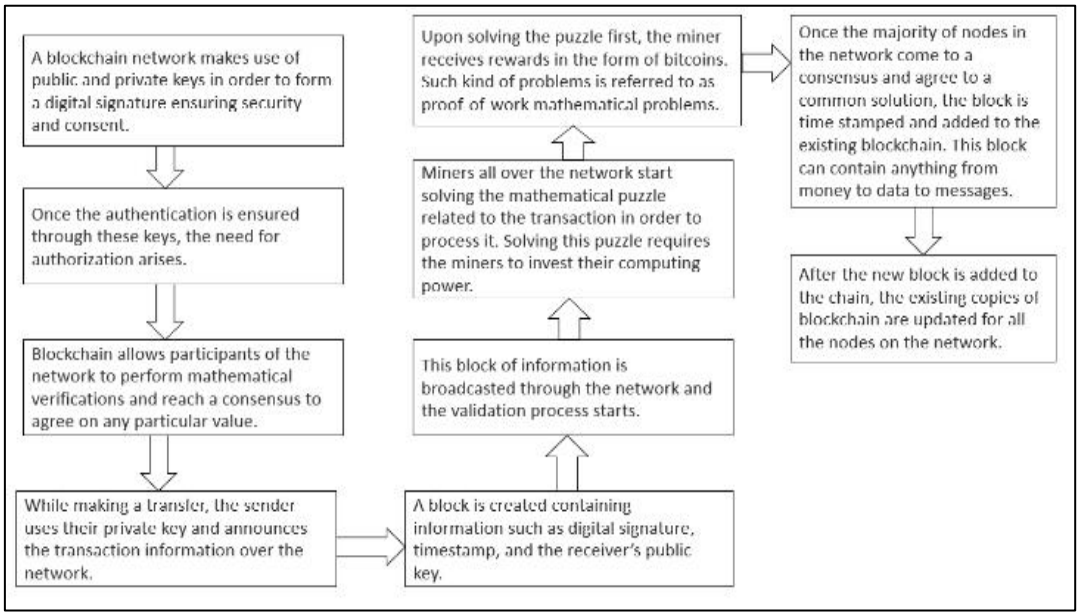

Fig 5. The overall process flow of Blockchain (Cryptocurrency Bitcoin has been considered)

Fig 6(a). Prediction of Blockchain market based on different regions [31]

So far, the most prominent attention to Blockchain technology has been received through cryptocurrencies.

Examples are Bitcoin, Litecoin, Dogecoin, etc. [32]. There are already existing blockchain-based applications in industry and the public sector like crowdfunding, tracking of goods in supply chains, Voting services, and many more [33]. Blockchain is vulnerable to various attacks '51% attack' happens. A rouge miner or user controlling more than half of the network's total hashing power can perform this attack. Still, Due to the immense attacking cost to perform, it is considered very unlikely for a long period. Another type of most major attack is the 'Sybil Attack. 'The

attackers can come out with several fake nodes that will appear genuine to their peers. These fake nodes take part in corrupting the network to validate unauthorized transactions and to alter valid transactions. All these can lead to DOS or DDoS. While considering our model, we have considered these situations. But since the size of SDN is very massive hence the total number of blocks will be huge. So, the possibility of a '51% attack' will be too expensive for a rogue user. Also, If you can detect the intruder by an early attention mechanism, 'Sybil' and '51% attack 'can be prevented [38-45]. In our idea, we have proposed a similar kind of thinking. In our case, nodes are intelligent and self-sufficient to make a decision. Blockchain also brings some negative impacts; blockchains require much computing power and energy [35]. For example, for Bitcoin alone, it had been calculated that by 2020 it might use as much energy as Denmark [34]. The central problem is that all transactions in the blockchain must be processed pervasively by everyone, and also everyone must have a copy of the global ledger. So, if we are proposing a blockchain-based architecture, we must find a solution that can decimate the energy consumption effect. One solution to this problem could be 'HoloChain,' where the application cell in the user has a chunk of code that will define to rule of the game. It's like DNA. These application cells are responsible for any action to be taken. Each of these applications has its ledger. It supports the local view of the system instead of the Global view which blockchain holds. Each transaction is monitored by a small set of randomly chosen peers, who store its transaction data, check it against their copy of the transaction rule, and broadcast an alert if they see anything wrong. The insertion time complexity for blockchain is $O(n^2)$, while Holochain is O (n log(n)), where n is the nodes number in the network. Also, 'Holochain' is infinitely scalable. So, it gives an added advantage [36,37]. It talks about an intelligent node with a local view. Our proposed solution for an SDN has tried to address the concept of 'Holochain' in this regard.

D. WHY BLOCKCHAIN LIGHT NODES?

As said earlier, the energy consumption of a blockchain node is very high, and due to complex execution, there may be a delay in the network. Most of the DoS or DDoS attacks are first initialized in the User plane for an SDN network. Knowing a mechanism that can take immediate action based on the transaction request before sending it to the user plane's control plane will generate more incredible value. Hence, we have incorporated the concept of lightweight blockchain nodes in our proposed hypothesis. The user plane data can be kept on a light node of the blockchain. It's needless to mention later, after any action taken by the lightweight node, the action course has to be broadcasted in the upper and lower layer or in the same layer later or at the same time. In the case of a light node, we have the most recent blocks. Whereas in a full node, we have the entire chain on your device. It is not required to download the whole blockchain. Light Weight nodes are connected to a server with a synchronized node, enabling users to work immediately. So, the time complexity of taking immediate action will be far better benefitting.

E. FOG SERVER

We have stated before that our model can achieve an improved performance considering low latency. The lightweight blockchain node on top of the Data plane addresses that. But to make it more efficient, we have brought the conception of Fog computing. Fog computing, also called Edge Computing, is mainly intended for distributed computing where numerous "peripheral" devices connect to a cloud-like SDN. These are the switches or routers. These devices will generate immense raw data (SDN, due to colossal network requirements for sustained traffic). Still, instead of forwarding all this data to remote cloud-based servers, they process the data locally. The idea behind fog computing is to reduce bandwidth requirements. Also, the same devices that generated the data process the data locally rather than remotely, the latency response is minimized concerning input [46-51].

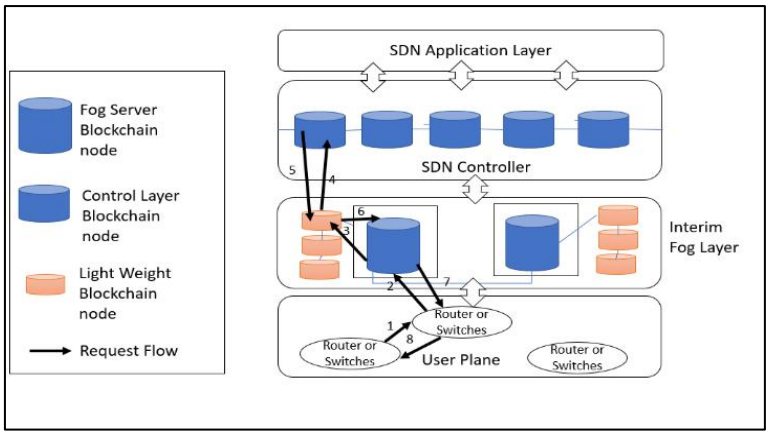

Fig 6(b). Prediction of Blockchain market based on different regions [31]

IV. METHODOLOGY

An event is deterministic if the previous physical event ultimately determines it. Nonlinear dynamics is the study of systems that are described by nonlinear equations of motion. The theory of nonlinear dynamical systems (chaos theory) deals with deterministic systems that exhibit a complicated, apparently random-looking behavior [18]. When DoS attacks are sufficiently strong, the trajectories of the state may leave the linearization region, which may in turn cause instability due to the nonlinearity of the dynamics leads to chaos in the network [19]. A tiny change in the state, as mentioned earlier, can cause crucial changes in the outcome of the dynamic system. This is known as the 'Butterfly Effect.' This highlights that the future cannot be predicted even in deterministic systems, entirely dependent on their initial conditions without any random elements. This is described as chaotic behavior or simply chaos [20]. Jianwen Chen et al. [21] had provided a concept based on artificial intelligence technology that exploits nearly complementary information of each node. They had divided two types of blockchain nodes based on average transaction number (ATN) 'Supernodes' and 'Randomnodes.' ATN has been trained by any DNN model like CNN, where its objective will be to predict the average transaction number of each node. One node is awarded a 'Supernode' as long as its rank is higher than a threshold value. So 'Supernodes' are nodes with more powerful computational capability, less network latency, more mining equipment. 'Random' nodes are nodes apart from 'Supernodes,' which guarantee the fairness of the network.

$$N = Super \cup Random \quad (1)$$

Our proposed method advocates a Multi-tenant intelligent brain that will be shared among all the blocks. Multi-tenant refers to an architecture where a single instance of the application is being shared. Now here, the Intelligent brain's training part will be done by data parallelism. The training data are split into non-overlapping chunks and fed into the model replicas of the workers for training. So, each blockchain node will have a local and a global view, and it makes a decision. Chonka et al. [22], in their paper, has suggested a DNN model where they had a state that DDoS traffic causes a strange attractor to develop in the pattern of network traffic; we have tried to amalgamate the idea with our prosed idea for detection of DoS in SDN based blockchain system. So now, this part of the intelligent brain inside nodes is self-similar. This means it's exactly or approximately similar to a piece of itself by its nature. We pick two types of blocks: B_s as 'Super Block' B_r as 'Random Block.' We pick B_r as a typical block where the moderate transaction happens below a threshold value and Bs where there is a high probability of attack traffic.

$$B_r+1=f(B_r) \quad (2)$$

$$B_s+1=f(B_s) \quad (3)$$

Where f (B) maps the nonlinear function of the dimension of the input variables, which is similar to the dimension of output variables. From (2) and (3), we can sequence of form

$$B_{r0},B_{r1},B_{r2},B_{r3}\ldots\ldots\ldots\ldots B_{rN} \quad (4)$$

$$B_{r0}+\Delta B_{r0},B_{r1}+\Delta B_{r1},B_{r2}+\Delta B_{r2},B_{r3}+\Delta B_{r3}\ldots B_{rN}+\Delta B_{rN} \quad (5)$$

$$B_{s0}+\Delta B_{r0},B_{s1}+\Delta B_{r1},B_{s2}+\Delta B_{r2},B_{s3}+\Delta B_{r3}\ldots B_{sN}+\Delta B_{rN} \quad (6)$$

The sequence (4) (5) are the orbit or trajectory of (2), representing standard transaction and changed transaction due to new transaction or sudden bursty transaction. A trajectory is a path tracked down by a changing body here, a transaction; an orbit is a periodically repeated trajectory. Equation (6) is the orbit or trajectory of the 'Random Node' transaction to the 'Supper Node' transaction, given in (3). Our assumption, in this case, is supernodes will hold the critical information of DoS. Now consider the two points in space, random Node (B_{r0}) and Super Node ($B_{s0} + \Delta B_{r0}$). We assume that transactions are associated with fixpoints which diminish asymptotically with ΔB_r (B_{r0}, t). We have also considered that in our model that at any time the random block orbit diverges exponentially but eventually settles, it is either due to a new transaction entering the system or a burst of legitimate transactions. This behavior is modeled in (5). If the function ΔB_r (B_{r0}, t) behaves 'chaotically' when a new transaction enters the blocks, the function changes to ΔB_s (B_{s0}, t). Based on the assumptions above, we study the mean exponential rate of divergence between these two close orbits (normal and new transaction to see if it is attack traffic) using the Lyapunov Exponent.

$$\lambda_{max} = \lim_{B\to\infty} \frac{1}{t} ln \frac{|\Delta\, Br(Br0,t)\,|}{|\Delta Br0|} \quad (7)$$

If λ_{max} <1, the transaction orbits attract a stable fixed point from when they diverge due to new legitimate transactions, or bursty legitimate transactions, entering the system. This means that the change in the transaction phase-space graph is not caused by DDoS attack traffic.

If λ_{max} =1, the transaction phase-space graph is in a steady state. This event means that the introduced transaction traffic has moved the similar transaction line up and down; it can be a new standard for detecting attack transaction traffic.

If λ_{max} >1, the transaction traffic orbit is chaotic and unstable, which means the nearby points will diverge to any arbitrary separation. This is a representation of attack transaction traffic that an attacker introduced into the system. This transaction traffic is considered to be DDoS

attack traffic and dropped by any neural network-trained filters.

We have previously stated that all the nodes in blockchain architecture will be self-sufficient as they have an internal intelligence driven from a shared global and local view; also, these nodes have decision-making capabilities that any DNN filters can train, hence in case DoS occurs, a node can self-sufficiently take the next course of action which will further curb the effect of DoS. The main objective while taking self-decision is to block itself for a particular type of transaction or from a specific type of user; a node needs to investigate the possibilities for rational behavior of the other nodes and self. This type of practice can be found in 'Game Theory.' It's a kind of a notion of equilibrium. The idea is that if somehow, the node can decide under the rules to choose a particular strategy, this is a sign of stability, and features associated with such a collective choice can be expected to be observed. Assume that there are n nodes and that the loss (Which can be expressed by a maximum utilization threshold- current utilization) for node a real-valued loss function gives me $(x_1,\ldots, x_n) \rightarrow C_i (x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ represents the strategic choices by the nodes. The set of strategies $x_1, \ldots, x_n$ defines a 'Nash equilibrium' if no node can benefit from a change of strategy provided the other node stick to their strategy. Since we have multiple nodes which will be in action with different strategies, whether to continue with the particular type of transaction or with a specific user, a mixed-strategy Nash equilibrium can be considered as we are working with multiple nodes. A mixed strategy action profile has the property that no single player or node can obtain a higher expected payoff (utility) according to the player's or node's preference overall. Still, this state has its issues as the stage increases; the outcome becomes inefficient. Hence, we have considered a Bayesian approach by assuming that each node may be of several types (based on scheduling strategies). A class specifies the information a node possesses regarding the system (global or local view). The resulting refinement of Nash's equilibrium is called a 'Bayes–Nash Equilibrium' (BNE). In case anyhow a node is unable to capture any local or global view data transaction. A Basian Nash Equilibrium can help to resolve the problem.

The overall algorithm looks like below:

1. *Transaction request receives from Switch/firewall to another Switch/firewall in Fog interim layer's lightweight node via Fog server node.*
2. *Evaluate λmax at interim Fog server node and in light node.*

IF $\lambda_{max}<1$:

i) *Request sent to a node of Control plane*
ii) *Guidance and acknowledgment received in Fog server node via lightweight node.*
iii) *Transmission happens.*
iv) *Each transaction will be determined based on 'Bayesian Nash equilibrium' depending on the state of other nodes as well.*

IF $\lambda_{max}=1$:

i) *Request sent to a node of the Control plane.*
ii) *Guidance and acknowledgment received in Fog server node via lightweight node.*
iii) *Transmission happens.*
iv) *Update an Alarm for a probable new standard of attack in every node.*

Else:

I. *Discard in Fog Interim layer. No need to proceed further in Control Plane.*

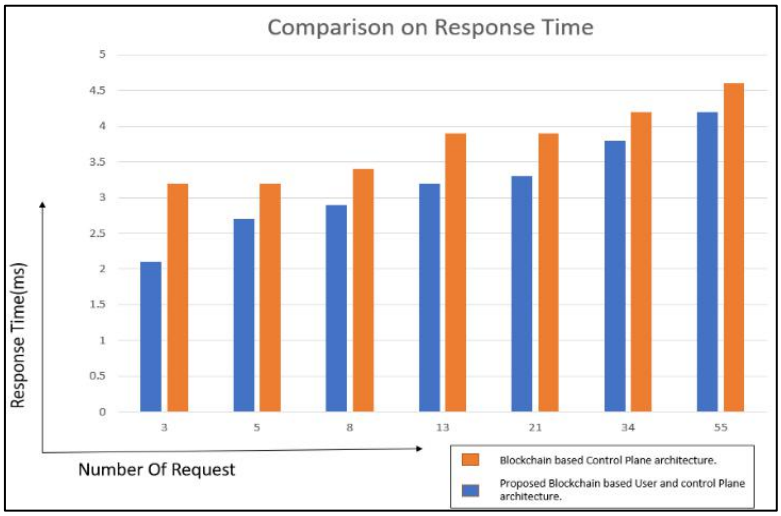

Fig 7. Comparison of response time

V. RESULT

We have presented the implementation detail, and now let's find out our proposed architecture's experimental results. We have carried extensive experiments to evaluate our approach in terms of accuracy, security, and efficiency. Our investigation shows that our proposed method's result is better in response time than SDN's decentralized control plane.

Also, our experiment shows the accuracy of our proposed system is more than 92%.

A CPU-based cluster of 10 Intel i7 1.6 GHz with 32 GB RAM servers and an SDN-based blockchain network with ten controllers/verifications and 990 request/response nodes has been used. The below result shows the delay in the network due to the proposed solution.

VI. CONCLUSION AND FUTURE WORK

In this research paper, we have developed an architecture and method for Software Defined Network to curb the impact of DoS and DDoS. Our central architecture is built on a Decentralized system. According to general design, our blockchain-based architecture of SDN comprises fog server-based blockchain light nodes in the data plane and a collection of full nodes in the control plane. Once the aggregated data packets in the gateway are forwarded to the data plane, comprised of OpenFlow-like switches, these packets are delivered into a layer consisting of the fog servers. This fog server holds a full blockchain node and is further distributed in lightweight nodes. All the nodes in this layer have the intelligence to decide whether to forward and discard the data packets. Decision-making criteria for these nodes are built based on chaos theory, and also, while working together, intelligent nodes can take decisions based on Basian Nash Equilibrium.

Table 1. Detection accuracy.

Packet arrived per seconds	Total Number of packet		Packet Classified		Detection Accuracy
	Normal Request	Flooding Request	Normal Request	Flooding Request	
15	250	40	252	38	95%
25	850	150	854	146	97%
35	1300	200	1109	191	96%
45	2500	400	2114	386	96%

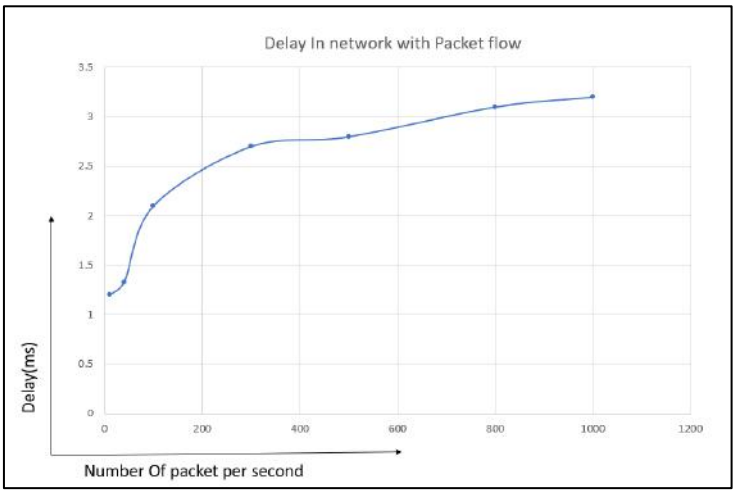

Fig 8. Delay response due to the proposed algorithm of DoS detection.

So further action takes place once a node in this fog layer decides to forward the data packet to the control plane layer, which is decentralized using full blockchain nodes. These nodes also are intelligent based on before mention aspects. So, if any intruder directly tries to access the control plane, blockchain nodes can take the correct decision where to forward or discard. Our filtering idea is based on a Deep neural network that can decide on certain parametric features associated with DoS and DDoS. DOS and DDoS parametric quality are evaluated by the measure of Lyapunov exponent, which helps characterize the various forms of synchronization in chaotic dynamics. Lyapunov exponents measure the growth rates of generic disturbance, in this case, DoS and DDoS, in a practice where linear equations can describe their evolution. After that, we considered that each node in our system would be involved in the Bayesian game. The reason is time→0(considering 0 latency in system); each node will have incomplete

information about other nodes. So, each node now will form a strategy based on Bayesian Nash equilibrium and take the further decision. The performances of the proposed architecture are evaluated in terms of delay, throughput, accuracy, response time, processing time, and security. The results of our performance evaluation demonstrate that compared to the previous work, our proposed architecture is more efficient and secure.

Next generation of DLT is 'Holochain'. In our future work, we want to implement an SDN network based on 'Holochain' as the overhead of blockchain can be drastically reduced via Holochain. Also, we want to create a holistic approach towards detecting other security concerns in SDN networks and try to provide an optimized solution for that.

REFERENCES

[1] Hu, Q. Hao and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2181-2206, Fourthquarter 2014, doi: 10.1109/COMST.2014.2326417.

[2] Abdelouahid Derhab, Mohamed Guerroumi, Mohamed Belaoued, Omar Cheikhrouhou, "BMC-SDN: Blockchain-Based Multicontroller Architecture for Secure Software-Defined Networks", Wireless Communications and Mobile Computing, vol. 2021, Article ID 9984666, 12 pages, 2021. https://doi.org/10.1155/2021/9984666.

[3] J. Soares et al., "Toward a telco cloud environment for service functions," in IEEE Communications Magazine, vol. 53, no. 2, pp. 98-106, Feb. 2015, doi: 10.1109/MCOM.2015.7045397.

[4] X. Zhiqun, C. Duan, H. Zhiyuan and S. Qunying, "Emerging of Telco Cloud," in China Communications, vol. 10, no. 6, pp. 79-85, June 2013, doi: 10.1109/CC.2013.6549261.

[5] 2021, https://www.sdxcentral.com/sdn/definitions/what-is-openflow/.

[6] M. Imran, M. H. Durad, F. A. Khan, and A. Derhab, "Toward an optimal solution against denial of service attacks in software defined networks," Future Generation Computer Systems, vol. 92, pp. 444–453, 2019.

[7] Mishra, Shailendra & Alshehri, Mohammed. (2017). Software Defined Networking: Research Issues, Challenges and Opportunities. Indian Journal of Science and Technology. 10. 1-9. 10.17485/ijst/2017/v10i29/112447.

[8] Raphael Horvath, Dietmar Nedbal, Mark Stieninger,A Literature Review on Challenges and Effects of Software Defined Networking,Procedia Computer Science Volume 64,2015,Pages 552-561,ISSN 18770509,https://doi.org/10.1016/j.procs.2015.08.563(https://www.sciencedirect.com/science/article/pii/S1877050915026988)

[9] arXiv:1905.04649v1 [cs.NI]

[10] Faridullah Amarkhil , Prashansa Taneja, 2020, A Research Paper of Security Enforcement Policy for (SDN) (WLAN) Software Defined Network, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT.) Volume 09, Issue 06 (June 2020)

[11] Papavassiliou, Symeon. 2020. "Software Defined Networking (SDN) and Network Function Virtualization (NFV)" Future Internet 12, no. 1: 7. https://doi.org/10.3390/fi12010007

[12] Bermbach, David & Pallas, Frank & Pérez, David & Plebani, Pierluigi & Anderson, Maya & Kat, Ronen & Tai, Stefan. (2017). A Research Perspective on Fog Computing.

[13] https://www.gartner.com/doc/2963217/rightsizing-data-center-network-

[14] Rahman, Gohar & Chuah, Chai Wen. (2018). Fog Computing, Applications, Security and Challenges, Review. International Journal of Engineering & Technology. 7. 1615. 10.14419/ijet.v7i3.12612.

[15] https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

[16] https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[17] Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Appl. Sci. 2019, 9, 1788. https://doi.org/10.3390/app9091788 AMA Style

[18] Dokoumetzidis, A., Iliadis, A. & Macheras, P. Nonlinear Dynamics and Chaos Theory: Concepts and Applications Relevant to Pharmacodynamics. Pharm Res 18, 415–42(2001).https://doi.org/10.1023/A:1011083723190

[19] Cetinkaya, A.; Ishii, H.; Hayakawa, T. An Overview on Denial-of-Service Attacks in Control Systems: Attack Models and Security Analyses. Entropy 2019, 21, 210. https://doi.org/10.3390/e21020210

[20] Andria Procopiou, Nikos Komninos, Christos Douligeris, "ForChaos: Real Time Application DDoS Detection Using Forecasting and Chaos Theory in Smart Home IoT Network", Wireless Communications and Mobile Computing, vol. 2019, Article ID 8469410, 14 pages, 2019. https://doi.org/10.1155/2019/8469410

[21] Chen, Jianwen & Duan, Kai & Zhang, Rumin & Zeng, Liaoyuan & Wang, Wenyi. (2018). An AI Based Super Nodes Selection Algorithm in BlockChain Networks.

[22] Chonka, Ashley & Singh, Jaipal & Zhou, Wanlei. (2009). Chaos theory based detection against network mimicking DDoS attacks. Communications Letters, IEEE. 13. 717 - 719. 10.1109/LCOMM.2009.090615.

[23] S. Boukria, M. Guerroumi and I. Romdhani, "BCFR: Blockchain-based Controller Against False Flow Rule Injection in SDN," 2019 IEEE Symposium on Computers and Communications (ISCC), 2019, pp. 1034-1039, doi: 10.1109/ISCC47284.2019.8969780.

[24] Wenjuan, LI., Weizhi, M., Zhiqiang, L., & Man-Ho, A. (2020). Towards Blockchain-Based Software-Defined Networking: Security Challenges and Solutions. IEICE Transactions on Information and Systems, E103.D(2), 196-203. https://doi.org/10.1587/transinf.2019ini0002

[25] Yazdinejad, R. Parizi, A. Dehghantanha, Q. Zhang and K. Choo, "An Energy-Efficient S.D.N. Controller Architecture for IoT Networks With Blockchain-Based Security" in IEEE

Transactions on Services Computing, vol. 13, no. 04, pp. 625-638, 2020. doi: 10.1109/T.S.C.2020.2966970 keywords: {blockchain;computer architecture;energy consumption;routing protocols;internet of things;authentication} url: https://doi.ieeecomputersociety.org/10.1109/TSC.2020.2966970

[26] Theviyanthan Krishnamohan, Kugathasan Janarthanan, Peramune PRLC, Ranaweera A.T (2020); BlockFlow: A decentralized SDN controller using Blockchain; International Journal of Scientific and Research Publications (IJSRP) 10(03) (ISSN: 2250-3153), DOI: http://dx.doi.org/10.29322/IJSRP.10.03.2020.p999

[27] C. Tselios, I. Politis and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2017, pp. 303-308, doi: 10.1109/NFV-SDN.2017.8169860.

[28] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba,A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer, "On scaling decentralized blockchains," in Proc. Int. Conf. FinancialCryptogr. Data Secur. Berlin, Germany: Springer, 2016, pp. 106–125.

[29] Fan, Stephen & Ghaemi, Sara & Khazaei, Hamzeh & Musilek, Petr. (2020). Performance Evaluation of Blockchain Systems: A Systematic Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3006078.

[30] https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020

[31] https://www.pwc.com/gx/en/industries/technology/blockchain/blockchain-in-business.html

[32] AUTHOR=Leible Stephan, Schlager Steffen, Schubotz Moritz, Gipp Bela TITLE=A Review on Blockchain Technology and Blockchain Projects Fostering Open Science JOURNAL=Frontiers in Blockchain VOLUME=2 YEAR=2019 PAGES=16 URL=https://www.frontiersin.org/article/10.3389/fbloc.2019.00016 DOI=10.3389/fbloc.2019.00016 ISSN=2624-7852

[33] Makridakis, Spyros & Christodoulou, Klitos. (2019). Blockchain: Current Challenges and Future Prospects/Applications. Future Internet. 11. 258. 10.3390/fi11120258.

[34] https://platformvaluenow.org/signals/problems-with-blockchain/

[35] Meva, Dr. Divyakant. (2018). Issues and Challenges with Blockchain: A Survey. INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING. 6. 488-491. 10.26438/ijcse/v6i12.488491.

[36] https://blog.holochain.org/satoshi-nakamoto-and-the-fate-of-our-planet-2/

[37] https://assets.ctfassets.net/sdlntm3tthp6/3h8Kkl1fEkk2KEMKiQQ2eC/d88343ceab28a70b0f121fc9c032b208/holochain__1_.pdf

[38] Sayeed, Sarwar & Marco-Gisbert, Hector. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Applied Sciences. 9. 1788. 10.3390/app9091788.

[39] Vitalik Buterin. Selfish Mining: A 25% Attack Against the Bitcoin Network. 2013. Available online: https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network/1383578440/

[40] IOTA. What Is IOTA? 2018. Available online: https://www.iota.org/get-started/what-is-iota

[41] Daniel Barta. IOTA: The Currency of Skynet. 2018. Available online: https://hackernoon.com/iota-the currency-of-skynet-281b6abaec5

[42] Bitcoin.com. What Is Bitcoin Double-Spending? 2017. Available online: https://www.bitcoin.com/info/what-is-bitcoin-double-spending

[43] Jon Matonis. The Bitcoin Mining Arms Race: GHash.io and the 51% Issue. 2017. Available online:https://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue

[44] Blockchain. Hash Distribution. 2019. Available online: https://www.blockchain.com/pools?timespan=24hours

[45] Alberto Garoffolo, Pier Stabilini, Robert Viglione and Uri Stav. A Penalty System for Delayed Block Submission. 2018. Available online: https://www.horizen.global/assets/files/A-Penalty-System-forDelayed-Block-Submission-by-Horizen.pdf

[46] Bonomi, Flavio (June 4–8, 2011). "Cloud and Fog Computing: Trade-offs and Applications. EON-2011 Workshop, International Symposium on Computer Architecture (ISCA 2011), San Jose, CA, USA". sites.google.com. Retrieved 2019-08-07.

[47] Janakiram, MSV (18 April 2016). "Is Fog Computing the Next Big Thing in the Internet of Things". Forbes Magazine. Retrieved 18 April 2016.

[48] Brogi, Antonio; Forti, Stefano (2017). "QoS-aware Deployment of IoT Applications Through the Fog" (PDF). IEEE Internet of Things Journal. PP (99): 1185–1192. doi:10.1109/JIOT.2017.2701408. ISSN 2327-4662. S2CID 2880664.

[49] Nikoloudakis, Y.; Panagiotakis, S.; Markakis, E.; Pallis, E.; Mastorakis, G.; Mavromoustakis, C. X.; Dobre, C. (November 2016). "A Fog-Based Emergency System for Smart Enhanced Living Environments". IEEE Cloud Computing. 3 (6): 54–62. doi:10.1109/mcc.2016.118. ISSN 2325-6095. S2CID 25475572

[50] Sarkar, S.; Chatterjee, S.; Misra, S. (2018). "Assessment of the Suitability of Fog Computing in the Context of Internet of Things". IEEE Transactions on Cloud Computing. 6 (1): 46–59. doi:10.1109/TCC.2015.2485206. ISSN 2168-7161. S2CID 3823420.

[51] https://en.wikipedia.org/wiki/Fog_computing