International Journal of Future Generation Communication and Networking
Vol. 13, No. 3s, (2020), pp. 1587–1593

Application of Blockchain in Software Defined Network

Praneeta Dumbre[1], Shailesh P. Bendale[2]
[1]*T.E. Student, Dept. Of Computer Engineering, NBN Sinhgad School of Engineering,Ambegaon,Pune-411041,*
[2]*Professor, Dept. Of Computer Engineering, NBN Sinhgad School of Engineering,Ambegaon,Pune-411041*

Abstract

With Technological advancement it has become necessary to construct a network which is centralized and can be controlled through various policies with maximum security. SDN being a software defined network is introduced to provide agility in network that is being widely used and to provide security to the SDN network we are using Blockchain. Blockchain is a trending technology which allows information to be distributed over a peer to peer network and not copied. Problems faced in providing security to SDN are the attacks like and privacy in the network. The first application of Blockchain was Bitcoin and crypto currency but its application is not limited to this two. There is a lot of work being done in Health-Care, Tourism, Finance, Automation and Management using Blockchain as core technology. To resolve this problem we use Blockchain Technology which will minimise the threats and give effective way of implementing this network. In this paper we are going to study collaboration of SDN and Blockchain together in a network and the applications which can be designed around this two technologies.

Index Terms: *Blockchain, SDN, Cyber Security, IoT, EVs*

I. INTRODUCTION

BLOCKCHAIN goes back to the time when crypto currencies were introduced in the market but now-a-days its application is not limited to crypto currencies or its famous application i.e. Bitcoin. Blockchain is a single word but if we separate it we get Block Blocks here means increasing list of records where each record acts like a block and is connect together in a network to form a chain thus giving its name i.e. "Blockchain". The concept of Blockchain was into market in 2008 but it origin goes in 1991 where it was introduced in an attempt to avoid the tampering of document timestamps.

The application of Blockchain was to introduce a transaction system where there is no place for financial institutions. Due to various functionalities like decentralization, anonymity, persistency and audibility it became wide spread technology in various fields like health-care, Internet of Things(IoT),finance, etc.[13].The advantage of this technology is the security it provides in any transaction done it's network making a secure technology by use of cryptography algorithm and the mechanisms of encryption and decryption. It is termed as the most powerful technology which can be used to avoid attack on network like the distributed Denial of Service attack (DDoS).Blockchain technology was built in such a way that there is no need of third party to handle and carry out the transaction for ourselves. We can carry out the transactions by directly meeting the concerned party and there is no need of managing web servers and databases by the third party.

Software defined Networks (SDN) is a new technology in the market which makes the network flexible and agile by making it as a programmable network. They are centralized in nature i.e. they contain a controller which acts as the intelligence behind all the operations being carried out in the network. The major problem behind this network or the threats to SDN are Distributed Denial of Service attacks and failure of the controller. This problem can be solved by collaboration Blockchain with SDN and distributing some functionalities over the network.
In this paper, we are going to discuss how the current systems in various fields of technology are making use of Blockchain and SDN. In this paper our major contribution is to give:

- Detailed idea about Blockchain and SDN technology

ISSN: 2233-7857 IJFGCN

- Research findings about the recent implementation of this two technologies
- New challenges present and the Future scope of this two technologies

The paper is divided into 4 sections: section II contains the background and brief idea about Blockchain and SDN technology, section III contains the research findings and discussion about implementation of both, section IV contains the Future challenges about both the technologies and section V concluded our paper with the overall summary.

II. BACKGROUND BLOCKCHAIN

Blockchain was basically introduced to serve as public ledger in crytocurrency transaction. In Harvard Business Review, Iansiti, Marco; Lakhani, Karim R. [1] said that Blockchain is a transaction medium in which is open and distributed ledger which can be used to carried out transaction in efficient manner with proper authentication and verification. Blockchain being a distributed ledger is also decentralized in nature which is its key feature. Decentralized here means that there is no third party to carry out the transaction which means there is peer to peer transaction.
Initially, Blockchain used the hash cash method where the blocks in the network were timestamped without needing any trusted authority to sign it. This design was implemented in bitcoin transaction as public ledger for all transaction carried out in a network. The data structure used in bitcoin is Merkel tree in which data is hashed for each transaction present in a block. In Merkel tree also known as Hash tree, every node with no child node is labelled with cryptographic hash of data block and every internal node is labelled with labels of its child nodes.

There are four types of Blockchain network-Public, Private, Consortium and Hybrid. Public Blockchain acts as an open network where anyone can join in the transaction where Private Blockchain has restricted access means u need to be invited by the network administrator to join the network. Consortium Blockchain is a semi-private network where there are controlled number of users but which works across different organizations. Hybrid Blockchain is combination of both centralized and decentralized network and its working might vary depending on the transaction and network architecture. Blockchain security method includes public-key and private-key cryptography. Public key in a Blockchain network acts as an address and the private key acts as a password which is given to the user to decipher the data.

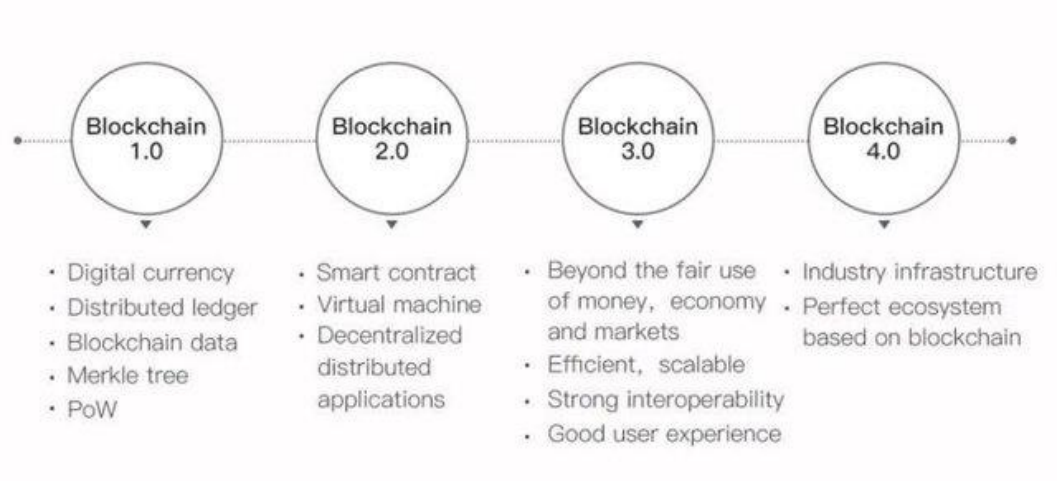

Fig 1.Evolution of Blockchain

SOFTWARE DEFINED NETWORKS

Benzekki.K et al. [2] said that Software-defined networking (SDN) technology is an approach in managing network which allows dynamic and programmatically efficient network configuration which improves network performance and provides advanced monitoring feature making it more like cloud

ISSN: 2233-7857 IJFGCN

computing over the traditional network. The introduction of SDN was made to replace the traditional network architecture to make it more agile and robust in nature. The disadvantage of traditional network was that it was not programmable in nature and not specific for implementation. We can say it was generic in nature but software defined network is programmable in nature and thus we can design it for specific work.

Any normal network contains two planes: the control plane and the data plane. The control plane is where the decision of traffic handling are made and data plane is where the actual advancing of data packets i.e. traffic takes place. In computer network this two planes are coupled together which affect the management of the network. So introduction of SDN has proposed a solution which says that we will separate this two layers from each other and have independent working. Here there is a controller which controls all the working in the networking while the other hardware devices like router, switches, etc. is used to transfer data packets to their destination as instructed by the controller. The architectural components of SDN include: SDN Application, SDN Controller, SDN Datapath and SDN Control to Data-plane interface and SDN Northbound Interfaces.

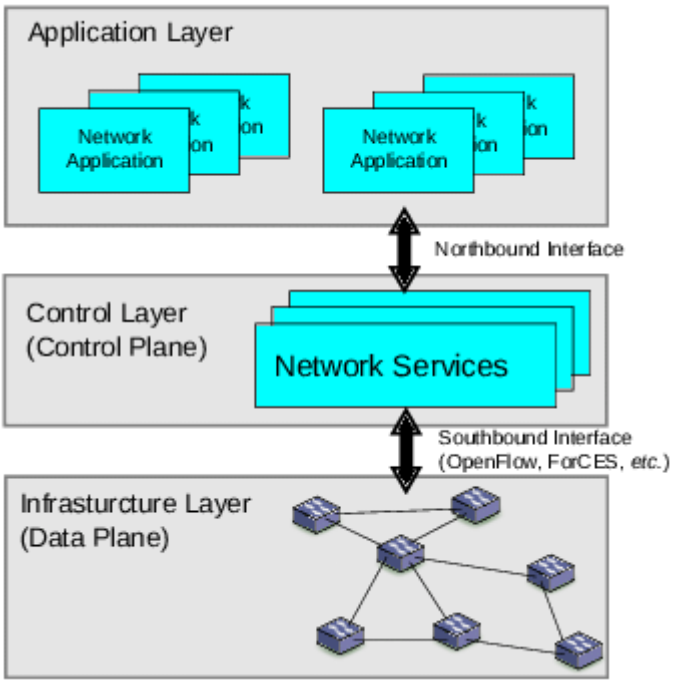

Fig 2.Architecture of Software Defined Networks

There is immense research going on in how to convert and introduce Software Defined network in the market but the major threat to this new technology is "Security". Diego Kreutz et al. [3] ,mentioned threats on SDN system as the DoS and DDos attacks like attacks on vulnerable switches, control plane communications, failure of controller, forged traffic attacks and lack of secure mechanism in control and management applications. According to research the most vulnerable element of SDN is the controller which centrally controls the whole network. Looking at the security aspect it's not feasible to have a centralized network as if the controller is out of action the whole network will collapse. To avoid this situation research is been done in a way where we can introduce decentralization in a centralized network, Here not all components of network will be decentralized but only the SDN security services will be decentralized so there is no need of centralized entity as it is in Blockchain Technology and help in improving security of SDN system.

III. RESEARCH FINDINGS AND DISCUSSION

Blockchain and SDN two being emerging technologies extensive research is being made in how to collaborate this two together in a single application. The complexity which lies in this collaboration is that both have contrary principles that is SDN is centralized network whereas Blockchain has

ISSN: 2233-7857 IJFGCN

decentralized network. So now we will see the application which have SDN and Blockchain collaboration used in different fields like IoT, Energy, Security, etc. This all research are related to studies done in past two years.

A. Yazdinejad et al. [4], have proposed a way in which they are using Blockchain and SDN architecture to make IoT devices energy efficient. Here Blockchain is used to provide necessary Security to the IoT device. They have tried making the network efficient by using cluster structure and implementing new routing protocol. The communication architecture they have used is P2P (Peer to Peer) and SDN controller. Here their major goal was to eliminate Proof of Work (PoW) and build distributed trust making Blockchain suitable technology for IoT Security. The objective behind this research was to how bring more agility in resource-constrained IoT device by adding SDN architecture and to enhance the existing Blockchain Technology. From this experiment the authors concluded that the performance of the IoT device increased by using routing protocol on cluster structure. It gave high throughput and efficient energy consumption than the traditional routing protocols (EESCFD, SMSN, AODV, etc.).

Guan Z, Lyu H, Zheng H, Li D, Liu J [5], proposed a SDN based system where we have distributed audit system for SDN based controller to avoid the untrusted environment in SDN and provide reliable deployment of the network. The shortcoming that the authors observed in the existing SDN network were that it was difficult to say that the quality of service while data transfer and the completion of transfer was guaranteed in the network. It was also difficult for the operators to perform audits based on the cost need in carrying out this operations. In the experiment they have changed the position of the controller and added it to the layer which performs the switching operation. They have used the consensus algorithm and the key generation method used is distributed type to make the distributed audit system. They have made use of consortium Blockchain as it is compatible with the distributed SDN system. The end result for this experiment was to generate log records in such a manner that they are untraceable and implement the audit function for controller which shoes the flow behavior. The algorithm used for the generation of distributed records is ECDSA signature algorithm. At the end of the experiments three conclusion were drawn that the effective signature on the log record depends on correctness of ECDSA digital signature, the generation of consortium Blockchain in the system depends on the validity of the distribution key generation protocol and assuming that both the algorithms are secure then the system can operate securely as the number of attackers in the system is reduced to 51%.The study is concluded by the integration of these different algorithms as mentioned above and the application of the system is stated as system for multi-operator auditing and cross-domain billing.

Chaudhary R et al. [6], proposed a new system called BEST: a Blockchain-based secure energy trading for the electricity-driven vehicle. The motivation behind this study was to build such a secure energy trading system which can be used for charging and discharging of the smart grids used by the electric vehicles. The use of Blockchain in this system is used to validate the request made by the EV's and working in a distributed format to avoid single point failure of the system. Here SDN system is used to reduce the network latency and improve Quality of Service (QoS) of the system[21]. The contribution of this study are first SDN-based vehicular system architecture which transfer data from global controller to EVs and vice versa. It also improves the system performance quality. Second, they have designed a miner code algorithm which is based on the vehicle mobility. It also calculates the energy required for the EVs, it's time for stay and energy pricing for the complete system. Third, a secure Blockchain design for energy trading allowing EVs to trade among themselves or with other utilities. Advantages of the proposed system after implementation were that it the system was lightweight and has minimal overhead of communication and all the computation processed on the network resources. The SDN system used enhances the Blockchain system efficiency by providing high network QoS. The future scope of this study includes implementation of this system of actual smart city energy grid and assess the prototype of the proposed study. This can help us know the scope of this system in real-world application.

ISSN: 2233-7857 IJFGCN

M. Boussard et al. [7], proposed a system naming STewWARD which is a SDN and Blockchain-based system used to evaluate the risk management involving IoT Devices. The motivation behind this study was the constant attack on data acquired by the IoT device and the security threats present for this devices. The most vulnerable network now-a-days is the home network or the home automation system which uses the maximum number of IoT devices and are the target networks to exploit[20]t. This study proposed that the user will ask its home controller to divide the network into software defined network slices and each slice will have its own risk assessment. There will be a trust score for each for each class of device which will be stored in Blockchain. Based on the trust score evaluation it will be decided which device will contribute to the crowd-sourced reporting by monitoring the device behavior and it's expected output. In the implementation they have used simple risk assessment test and some crowd sourced report and evaluated how the controller based on the trust score will connect or disconnect a device from a network slice having certain trust score. This system is majorly beneficial to home networks to reduce the attacks on the personal data and community by providing data to identify the emerging threats.

Huo L, Jiang D, Qi S [8], proposed a system for using Blockchain to manage the traffic on a software defined network. As the most vulnerable component of a software defined network is the controller they have introduced Blockchain as a measurement framework to calculate the risk and consistency of the data in the network. To measure the traffic flow they have collected the data of coarse-grained and fine grained traffic flow and model the network traffic as an ARIMA model. They have introduced a objective function which is NP-hard in nature which contains a heuristic algorithm to obtain the optimal solution of the fine grained measurement. They have also conducted simulations to validate the study and prove its efficiency and feasibility.

J. Gao et al. [9],the study has been proposed of how to used SDN and Blockchain system in Internet of Vehicles(IoV) for Fog computing and 5G.Here SDN is used to make network management more smooth and have high performance while Blockchain is used to provide to ensure trust between networking platforms. S. R. Basnet and S. Shakya [10], show the simple study of how Blockchain is used to provide security to the software defined network. They have used Mininet emulator for simulating the SDN network topology. For the storage purpose they have used OpenStack and OpenDayLight controller is integrated with it. For Blockchain they have used Pyethereum and Ethereum platforms for testing and implementation. To create contracts for Blockchain they have used Serpent programming which is same like Python but is used in real time interactive multimedia system. They have built two Blockchain networks and connected it to OpenStack controller and passed data over the network. Each node in the network contains public and private key and the encryption and decryption of data takes place according to the rule of cryptography.

IV. FUTURE CHALLENGE AND DIRECTIONS

As we have studied the different fields where we can use the collaboration of Blockchain and SDN together there are still some shortcomings in both the technologies which are to be explored. SDN has major issue of security as when we separate the data and control plane the working gets segregated and the components are more exposed to attack. Some of the shortcomings found in an SDN and Blockchain system according to researcher are:

- T. Alharbi, M. Portmann and F. Pakzad [12], they have referred to vulnerability of the SDN controller to Link Fabrication attack where the topology of the network or its view can be completely hampered by injecting a spoofed LLDP packet in the network. The solution to this problem is proposed as we can use Blockchain and distribute the LLDP Packet authentication between the network devices to make sure that no spoofed packets enter the network [11].
- T. Alharbi et al. [13], the implementation of Address Translation Protocol is also not secure over SDN.SDN is prone to ARP attack where the attacker will manipulate or change the ARP cache with fabricated information which might lead to a DoS attack[11]. We can apply the technique of distribution of packets among SDN hosts to avoid the attack.

ISSN: 2233-7857 IJFGCN

- T. Alharbi ,M. Portmann [14], the SDN virtualization is said to be prone to attacks as the number of components increases. Components here refer to running of multiple SDN controllers over the same network. This increases the complexity of the system.
- Chinmay Dharmadhikari, Salil Kulkarni, Swarali Temkar, Shailesh Bendale [15],have made a detailed study of how a DDoS attack affects SDN.They have also discussed various types of DDoS attacks methods,and algorithms for detection and mitigation of DDoS attack on SDN.
- Many studies have been proposed where the security threats in SDN are addressed by different technologies as AI in 5G which uses SDN architecture [16] and Machine Learning [17] but now we have to think of the way in which we can implement all this methods proposed using Blockchain.
- Blockchain first shortcoming is the complexity of the network. It is its feature as well as disadvantage it requires more management and thorough knowledge. The complexity of network also decides its usage. Companies and finance institutions are going for complete distributed network but for hybrid network which increases the complexity.
- The High energy consumption for Blockchain network is also a shortcoming in Blockchain implementation. Extensive study is needed to get a solution of how to implement application which will require less energy and resources but give efficient output.
- Scalability is also a limitation to Blockchain implementation. Scalability here means the number of transaction which are carried out in single network is less. For Blockchain only 7 transaction are possible at one time and the validation of each transaction takes a lot of time to be received. Blockchain works on Proof-of-Work but it is slow. Proof-of-Stake is an alternative to speed up the transaction but it's not ideal solution for distributed Blockchain system.

V. CONCLUSION

Software Defined Networks has brought a new way in which a network can be designed and made efficient. The control of the complete network is shifted to a single entity which is the controller and thus a centralized network is created. Although there are shortcomings to the implementation of SDN on large scale due to its vulnerabilities to different cyber-attacks. Blockchain is a technology which works on decentralization and distribution of data over the network. There are different types of network in Blockchain which are used in modern day application to make the applications more efficient and optimal. In this paper we have discussed how this two different technologies were merged together for different applications and how this both technologies complemented each other in different ways. Extensive research is being made in how to avoid the attacks in SDN based system and how to protect the components in network from potential attacks which might harm the data over the network. Thus this paper has given us the basic understanding of SDN and Blockchain ways of utilizing the feature of Blockchain in providing solution to the security problem of SDN and have development in making applications with SDN architecture which are secure and reliable.

REFERENCES

[1] Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017.

[2] Benzekki, K., El Fergougui, A., and Elbelrhiti Elalaoui, A. (2016) Software- defined networking (SDN): a survey. *Security Comm. Networks,* 9: 5803– 5833. doi: 10.1002/sec.1737.

[3] Diego Kreutz, Fernando M.V. Ramos, and Paulo Verissimo. 2013. Towards secure and dependable software-defined networks. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (HotSDN '13). Association for Computing Machinery, New York, NY, USA, 55–60. DOI:https://doi.org/10.1145/2491185.2491199

[4] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang and K. R. Choo, "An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security," in IEEE Transactions on Services Computing.

[5] Guan Z., Lyu H., Zheng H., Li D., Liu J. (2019) Distributed Audit System of SDN Controller Based on Blockchain. In: Qiu M. (eds) Smart Blockchain. SmartBlock 2019. Lecture Notes in Computer Science, vol 11911. Springer, Cham

ISSN: 2233-7857 IJFGCN

[6] Chaudhary, R., Jindal, A., Aujla, G. S., Aggarwal, S., Kumar, N., & Choo, K.-K. R. (2019). BEST: Blockchain-based Secure Energy Trading in SDN-enabled Intelligent Transportation System. Computers & Security. doi:10.1016/j.cose.2019.05.006

[7] M. Boussard, S. Papillon, P. Peloso, M. Signorini and E. Waisbard, "STewARD:SDN and blockchain-based Trust evaluation for Automated Risk management on IoT Devices," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 841-846.

[8] Huo, L., Jiang, D., Qi, S. et al. A Blockchain-Based Security Traffic Measurement Approach to Software Defined Networking. Mobile Netw Appl (2020). https://doi.org/10.1007/s11036-019-01420-6

[9] J. Gao et al., "A Blockchain-SDN enabled Internet of Vehicles Environment for Fog Computing and 5G Networks," in IEEE Internet of Things Journal.

[10] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 2017, pp. 720-725.

[11] T. Alharbi, "Deployment of Blockchain Technology in Software Defined Networks: A Survey," in IEEE Access, vol. 8, pp. 9146-9156, 2020.

[12] T. Alharbi, M. Portmann and F. Pakzad, "The (in)security of Topology Discovery in Software Defined Networks," 2015 IEEE 40th Conference on Local Computer Networks (LCN), Clearwater Beach, FL, 2015, pp. 502-505.

[13] T. Alharbi, D. Durando, F. Pakzad and M. Portmann, "Securing ARP in Software Defined Networks," 2016 IEEE 41st Conference on Local Computer Networks (LCN), Dubai, 2016, pp. 523-526.

[14] T. Alharbi and M. Portmann, "The (In)Security of Virtualization in Software Defined Networks," in IEEE Access, vol. 7, pp. 66584-66594, 2019.

[15] Chinmay Dharmadhikari, Salil Kulkarni, Swarali Temkar, Shailesh Bendale ," A Study of DDoS Attacks in Software Defined Networks" (IRJET) 2019.

[16] Siddhant Shah, Shailesh Bendale, "An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era.", ICCUBEA, 2019

[17] Shivam Tiwari,Vanshika Pandita,Samarth Sharma,Vishal Dhande,Shailesh Bendale,"Survey on SDN based network intrusion detection system using Machine Learning Framework",(IRJET) 2019.

[18] A. S. Patil, P.S. Jain, R.G. Ram, V.N. Vayachal and S.P. Bendale,"Detection of distributed denial of service attack on SDN", (IRJET) 2018.

[19] MA Patil, MP Jain, MR Ram, MV Vayachal, SP Bendale,"Software Defined Network:DDoS Attack Detection",(IRJET) 2019.

[20] Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications.

[21] Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2017). An optimal routing algorithm for internet of things enabling technologies. *International Journal of Rough Sets and Data Analysis*, *4*(3), 1–16.

ISSN: 2233-7857 IJFGCN