Research Article

A Study on the Application of Blockchain Technology based on Direct Acyclic Graph in IoT environment

Dr.Ho-Kyung Yang [a], Dr.Hyun-Jong Cha [b], Dr.You-Jin Song [c*]

[a] Division of Information Technology Education, Sunmoon University, KOREA
[b] Department of Multimedia Science, Chungwoon University, KOREA
[c] Department of Information Management, Dongguk University, KOREA
Corresponding Author: You-Jin Song, **email:** song@dongguk.ac.kr

Abstract: U The services provided by the Internet of Things create new values, enabling communication with objects rather than communication between people. However, problems arise due to security of services or limitations in network operation. Recently, research is underway to help block cloud (Block Cloud), a platform combining SCN(Service-Centric Networking) and blockchain, provide services rapidly based on instances rather than traditional IPs and resolve trust in services through consensus algorithms. In addition, the Internet of Things network has been proposed as the Fog Computing environment, an environment suitable for real-time processing of information in the context of traditional cloud computing. In this paper, to introduce and utilize this information to expedite the processing of services for the Internet of Things, IOTA, the third generation block chain based on DAG, is applied to the block cloud and the new Internet network structure that requires real time is based on Fog computing. Also, we propose a basic model of object block chain and propose electric vehicle application service based on this basic model.

Keywords: Block Cloud, Fog Computing, SCN, Blockchain-based Internet of Things, Tangle

1. Introduction

According to the trend of 10 strategic technologies in 2018, Internet of Things (IoT) has emerged as an area that could create new value through interaction between the reality and a virtual world in the Fourth Industrial Revolution. It expected that approximately 21 billion devices would be connected each other by 2020, which means that our society will soon enter the era of Hyper-Connected Society **(CeArley, Burke, Searle and Walker, 2016)**. In a hyper-connected society, everything including people, things and even space is connected through Internet and information is generated, shared and used under such connected Internet environment. Communication between things connected through Internet, as well as people, creates a variety of value-added services, and provides innovative service in industrial areas **(Dawson, Eltayeb and Omar, 2016; Kim, 2019)**. Currently, various studies on Internet of Things are progressing to build such system and have attracted significant and strong attractions **(Vermesan and Friess, 2015; Choi, 2014; Yin, guo, Wang, Jiang, Lyu and Xing, 2018; Jang and Shin, 2020; Moon, 2020; Park and Cha, 2019)**.

The basic networking structure of Internet of Things is designed in a cloud computing method with a CS(Client-Server) structure in which a client sends information and a server processes it **(Hwang, Kim, Lee and Jung, 2017)**. However, A structure that receives a large amount of information in real-time and processes it at centralized server makes load concentrate to a server and places limitations on scalability, cost and size of a structure to process information **(Oluwatosin, 2014; Arsenio, Serra, Francisco, Nabais, Andrade and Serrano, 2014)**. Therefore, CISCO introduced the Fog- Computing IOx platform with a distributed network structure, escaping from cloud computing. In this platform, clients do not send data to a server directly and the data is received and processed at the middle point to improve data processing rate and server overload issue **(Butler, 2018; Saad, 2018; Jung, Lee and Jung, 2020)**.

Service provided in a network is also changing and being diversified from a traditional host-oriented environment. In the previous method, a server searches and provides a requested service, based on network information (including an IP and a port number of a supplier. SCN (Service-Centric Networking) that provides information based on service IDs and instances allows rapid searching and processing of service to be requested in real time because a router searches, based on service instance, rather than a location of specific host that providing service **(Griffin et al., 2015; Gasparyan, Corsini, Braun, Schiller and Saltarin, 2017)**.

A new method to improve service reliability has been proposed with blockchain technology. Bitcoin, the representative blockchain project, has attracted strong attention of people because it suggests no need of a central agency, and introduces P2P based network, which is a decision-making process through consensus between issuers **(Nakamoto, 2019)**. However, issues relating to transaction delay time, cost and protection of anonymity have been raised. Although IBM introduced Adept as a platform adopting blockchain technology in the IoT environment that allows many connected devices to join a network, there are still many studies in progress to deal with such issues mentioned above **(Panikkar, Nair, Brody and Pureswaran, 2015)**.

Recently, Block Cloud announced an IoT network integrating SCN and blockchain technology, called as Block Cloud. Block Cloud provides portability and scalability of a network, adopting SCN based network structure. In addition, the technology uses the blockchain system to verify trustiness of service through a distributed trust system **(Ming et al., 2018)**.

This paper introduces and uses Block Cloud and applies DAG based third generation blockchain IOTA to Block Cloud to quickly process IoT service. Then, it a proposes a new architecture to operate Block Cloud in a fog computing method, which is more suitable for IoT network structure as IoT requires real-time interaction. Furthermore, the study presents a basic model of IoT blockchain and proposes electric vehicle application process based on the basic model **(Atzori, Iera and Morabito, 2010)**.

In chapter 2, relevant researches forming the environment of this study such as IoT and fog computing, SCN and blockchain are explained. Chapter 3 describes proposal of this study for DAG type IoT blockchain. Chapter 4 presents a service model that applies the proposal to electric vehicles. In the conclusion, importance of this study and future direction of research are presented.

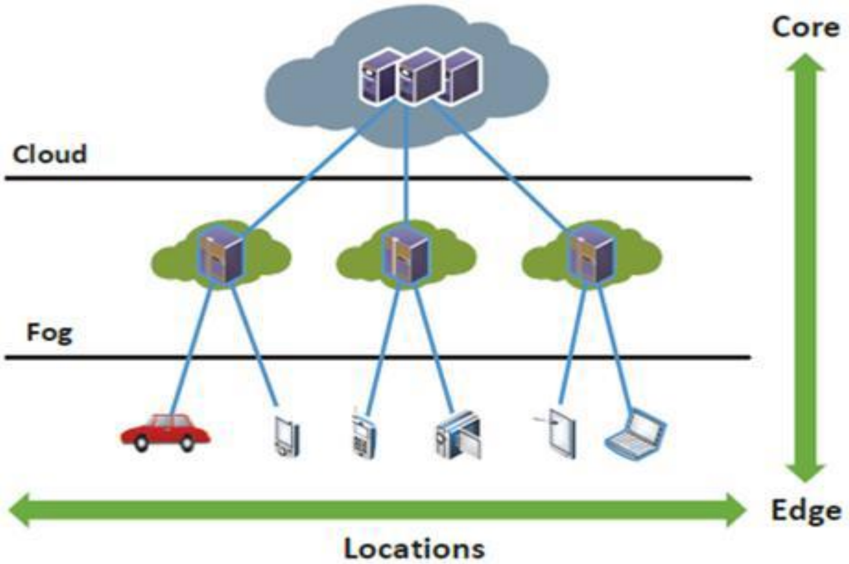
2.Related Works

In this section, we introduce basic concepts of block cloud, fog network, SCN network, and object block chain, which are core technologies needed for thesis.

2.1.Internet of Things and Fog computing

The concept of Internet of Things (IoT) started from the concept of Ubiquitous Computing. The word Ubiquitous came from Latin and means 'Being everywhere at once, omnipresent'. Ubiquitous technology refers to a technology that creates new value by communication and interaction between people and things, without spatial and temporal restrictions. A machine could be operated only be a person during previous periods. Now, a machine can provide people with information due to developed intelligence and automation of machines. IoT is called as 'communication network between things', accommodating such technologies.

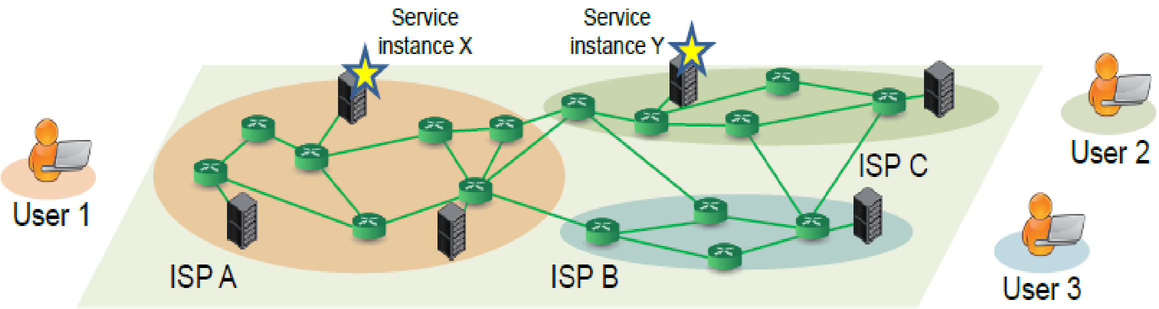
Figure.1 Fog Computing



Fog Computing solves latency issues caused by geographical features by introducing a fog near the edge of network that is placed at a position for quick processing of service requested to a cloud server. Fog computing has a structure with advantage of mobility that allows people to use the service at any time any place. Fog computing processes information in a distributed manner, which was processed at a central server before. Therefore, it is suitable to process a large amount of information exchanging between devices, which makes fog computing valuable element for IoT network. As a result, many researches on IoT network system using fog computing are in progress (Saad, 2018; Atlam, Walters and Wills, 2018). However, fog computing has some privacy issues and Man-in-the-Middle Attack issues and many researches are in progress to deal with such issues **(Stojmenovic and Wen, 2014)**.

2.2.SCN(Service-Centric Networking)

Figure.2 Process of SCN



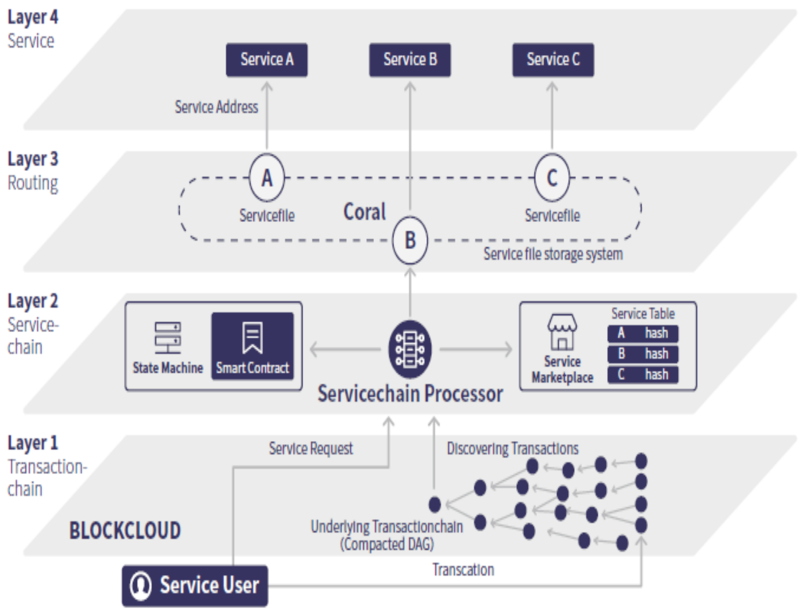
SCN (Service-centric networking) is a new network structure that changed host address based service to non-host-centric service in a large network. SCN provides network users with a solution of QoS restrictions, high bandwidth and latency in communicating with a certain host to have service. Refer to Figure 2, for example. there are many hosts that provides the same service in Area A, B and C of the network. When User 1 requests to measure traffic near an autonomous vehicle (Service X in Figure 2), a router searches the best service provider near User 1 in an optimized path, among service providers who have the same instance as User 1's request. Therefore, SCN allows users to request and use a service under the best demand and communication environment for them. It is also important to note that clients can use service, without connection with a certain host that provides service **(Griffin et al., 2015; Gasparyan, Corsini, Braun, Schiller and Saltarin, 2017)**.

2.3.BlockCloud

Blockcloud refers to a new type of cloud server platform that combines features of SCN and blockchain. Host centric service processing in an existing network has been improved to a network that can provide service instances with mobility and scalability using SCN. Trust to unclear service and service providers has been improved by adopting blockchain structure where trust can be obtained by consent of network participants. Let's try to explain the structure of blockcloud, referring to Figure 3. Blockcloud consists of total 4 layers. In the transaction chain layer, transactions requested to blockcloud are encoded in a transaction form and uploaded to the blockchain. If a transaction is approved, service requested by the transaction is verified and processed in the service chain layer. Service is processed by a service chain processor and saved into a database that contains overall status information according to change of blockchain given.

Currently, blockcloud defines two types of status information; overall service management system and service matching and price estimation system. In addition, it creates Smart Contract by matching service to a certain provider. Then, it provides information required for service routing so that service is implemented when contractual conditions provided by a user and a service provider are matched. In the routing layer, service is routed to a corresponding path when trustiness of service is verified at two layers mentioned above. Routing information is saved to a service file. A service name and a hash value are saved and managed in pair at the service chain layer. Then, such information is saved as a service file in the routing layer. In the service layer, actual service is provided to a user, and all services are signed by the signature key of a service owner **(Ming et al., 2018)**. This study proposes a new blockcloud model based on fog computing to solve bandwidth and latency issues inherent to existing cloud computing network structure and provide physical environment for IoT service architecture requiring real-time interaction, using blockcloud architecture presented in **(Ming et al., 2018)**.

Figure.3 BlockCloud Architecture



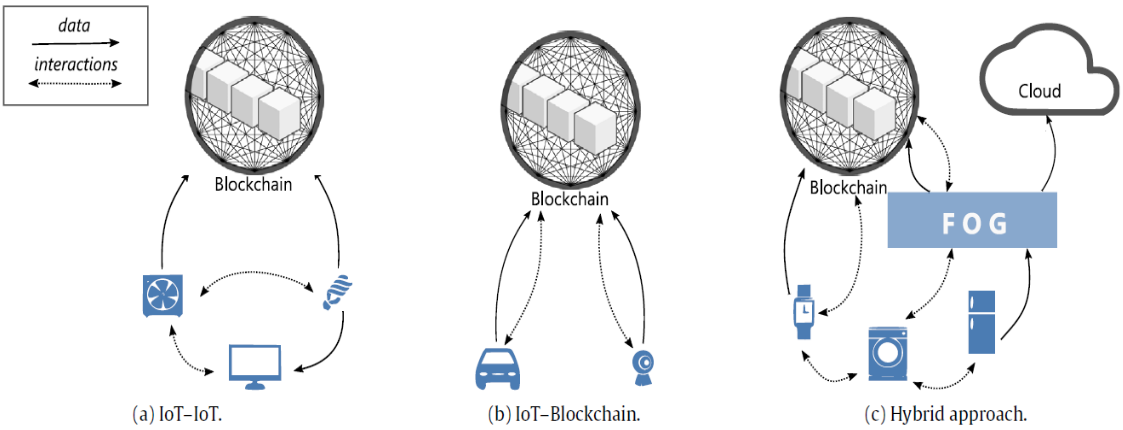
The basic model of BIoT consists of IoT devices, a data owner, a blockchain (and fog) network and cloud, as shown in Figure 3.

IoT Device.

IoT devices collect and send data to the network layer (e.g. cloud or other applications). IoT devices also conduct data collection, preliminary processing, encryption (if supported) and transmission. IoT devices generally allow remote access grant and order processing. If it is required to request data from other devices, such request should be published to the cloud or the data owner.

Figure 4 shows the application structures of IoT and the block chain.

Figure.4 Application Structures of IoT and Block Chain



Data Owner.

Data owners are classified as administrators and general data owners. Therefore, there are many data owners. Administrators have responsibility to investigate participants. When a data owner has access data request from other IoT devices, he/she should authenticate ID before making a response.

Blockchain & Fog Network.

This architecture uses a permitted model (e.g. hyperledger fabric). Particularly, security of a model is guaranteed under assumption that most participants are honest, and the issue is difficult to deal with. In other words, the average time for an attacker to solve an issue is significantly less than the time for information to be distributed through a network. Consensus Algorithm of the system is Practical Byzantine Fault Tolerance (pBFT), rather than Proof-of-Work, which is used for bitcoin. Fabric includes verification node (to verify transactions) and order node (to pack a verified transaction into a block) When a node receives a transaction (by request of a cloud or a data owner), it verifies the transaction and pack it into blockchain (Buterin, 2014; Buterin, 2018).

A fog network is a method to realize IoT proposed by CISCO. A fog network has a node to process data created at a device in real-time, like a station, and transfers only data that requires computing power to a cloud. If every data needs to be uploaded to a cloud through a network to process it, it is impossible to take an immediate action to provide users with valuable service because of latency. While fog computing can control data, it is difficult to verify whether a device is certified or not. To deal with this issue, an authentication code for each type of devices can be uploaded to blockchain to verify a device. In addition, security can be improved through attribute-based encryption, proxy re-encryption and distributed encryption method.

Cloud.

A cloud saves data of an encrypted device, transfers a transaction to a blockchain network and searches authority of a device, if requested from an IoT device. In other words, a cloud monitors a blockchain network and makes a response to data requested.

4.Application of DAG IoT Blockchain

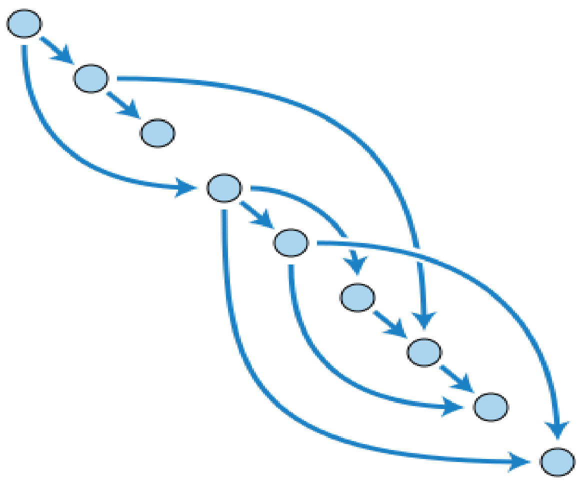
4.1.DAG Blockchain

While the first and the second generation of blockchain has linear structure, IoTA has non-linear blockchain. Due to the non-linear structure, it can process all transactions in parallel. Therefore, transaction speed increases if there are more issuers. Particularly, all previous blockchains had both miners and issuers. In IoTA, all issuers can equally approve and issue transactions. IoTA operates a transaction system based on DAG structure, which is called as Tangle **(Serguei, 2017)**.

DAG.

DAG (Directed Acyclic Graph) is a non-cyclic graph. As can be seen in Figure 5, the peak of a graph is connected to the peak of other graph in a direction. However, there is no cycle and it cannot return to itself through any path. Tangle uses the DAG's directionality among the transactions accumulated over time to select the tip based on the weight and reliability of the specific transaction **(Li et al., 2019; Serguei, 2017)**.

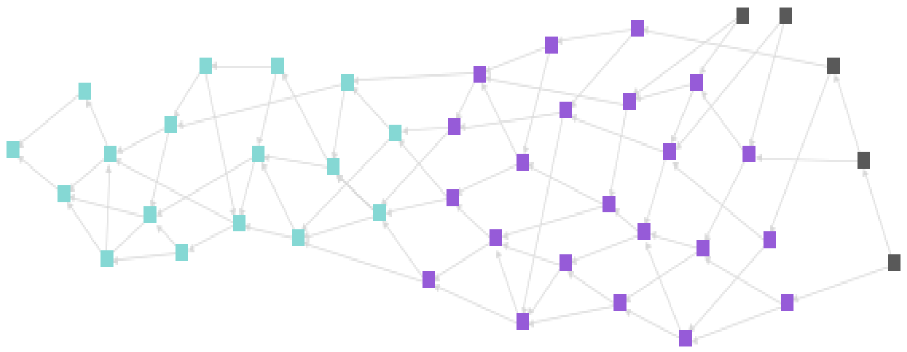
Figure.5 DAG Graph



Tangle.

For issuers to request a transaction in Tangle, they should approve two previous transactions. A transaction is selected by Tip Selection Algorithm (TSA). According to TSA, a transaction is randomly selected by its accumulated weight. To approve a selected transaction, a user who requests a transaction should have PoW (Proof of Work), Although the calculation process is similar with that of blockchain, actual amount of calculation to be required is not much. In addition, all issuers can proceed a transaction without a fee because one of the conditions to approve a transaction is no fee. Therefore, this is a transaction structure optimized for M2M and micro payment, which do not require high calculation capacity and any fee **(Serguei, 2017)**.

Figure.6 Tangle(DAG)



As can be seen in Figure 6, there are three types of transactions conducted in a Tangle network; completely confirmed transactions, not confirmed transactions and tips, which are decided by a confirmation level. In other words, the types are decided according to the number of direct or indirect approvals on previous transaction by newly generated tips.

Figure.7 IoTA Overview

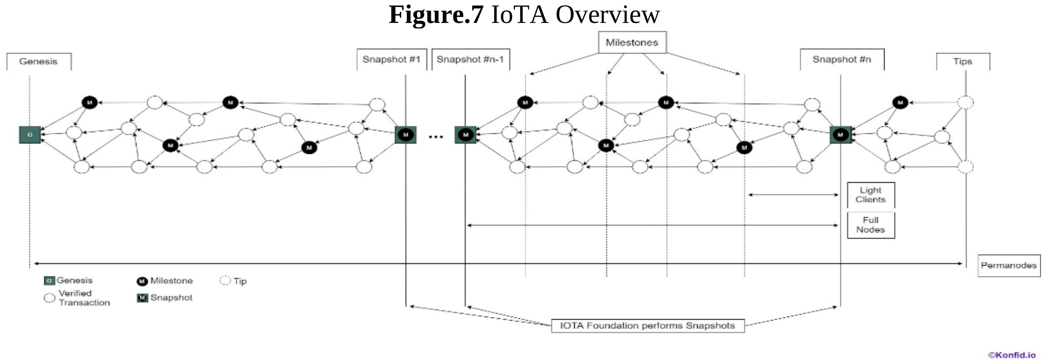


Figure 7 shows methods to maintain a normal transaction system in a Tangle network. Currently, IoTA Foundation does not disclose the number of traders who are participating in and the amount of transactions happening in a Tangle network. Transaction units are small and processing time is short when the number of participants in a network is small. If a malicious user takes an advantage of this factor and take a certain percentage of transactions happening in the network, transactions between other users could not be properly approved. Therefore, IoTA Foundation generates a certain transaction called as Milestone every two minute at a coordinate node to find whether transactions happening in a network is properly approved. Snapshot is a method to prevent overload on a large network. It removes a part of Tangle network when a certain period of time passes and saves a necessary part of user information for the removed network. As a result, an issuer does not need to save all status information of Tangle network. This paper creates a new type of service structure that allows rapid change from fog computing based blockcloud model, as described in Chapter 2, to IoT centric service requiring real-time transactions, adopting DAG based third generation blockchain IoTA.

4.2.Application Models

In this chapter, the third generation blockchain DAG based IoTA is applied to blockcloud and IoT centric network structure is designed, based on fog computing. Such structure shall meet the following requirements. Scalability of Transaction.

- Processing Service in Real-time
- No Fees
- Service-based Communications
- Offline Processing Service

The first requirement is ‘scalability of transaction’. To make and approve a transaction in blockchain, a special node, called as a miner, should complete a special process, called as mining, However, IoTA allows unrestricted transactions. Therefore, it has advantages in a large amount of transactions.

While the first and the second

The second requirement is 'Processing service in Real-time'. While existing cloud based service, processing is only available when a client and a sever are connected, fog computing based service processing allows immediate access from a near location to process service.

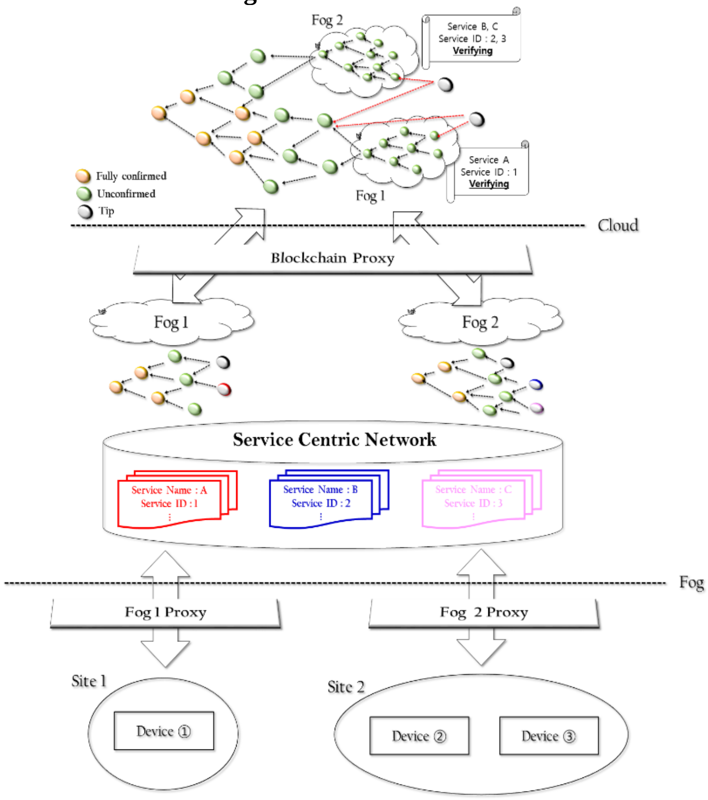
The third requirement is 'No Fee'. People who make a transaction must approve another transaction to obtain approval of their transaction in IoTA. Proof of Work process, which is similar with that of blockchain, is required to approve a transaction. However, all participants can approve a transaction with no fee because one of the conditions to approve a transaction is 'a role with no fee' and a job does not require complex calculation. Therefore, this is a system optimized for micro payment.

The fourth requirement is 'Service-based Communication', in which a service router searches and provides a service path requested by a client through a SCN network, focusing on service instances. Due to this characteristic, rather than connecting to a certain host, the range of host to provide service is widened and quick search is available.

The last requirement is Offline Processing Service. IoTA has a Tangle Structure and can create an offchain tangle (flash channel). A large amount of transactions processing can be available without uploading a transaction from a main Tangle. Under communication environment in which different devices have different protocols, offline data processing is inevitable. From this point of view, IoTA allows quick processing of IoT service by applying fog computing based blockcloud.

Model Design.

Figure.8 Model Overview



For overall process in Figure 8, when a device in IoT, a sensor node, requests service, service is transferred to a fog node that is searching a signal of sensor node through a near fog proxy. The service is delivered through SCN network in a form of packet that containing the service name and ID and saved as Tangle network transaction in a fog node. Once trustiness of service is verified, a sensor node prepares to receive service from a service provider's node, on the basis of routing information. After that, Tangle information formed at a fog node is transferred to blockchain of a cloud server through a blockchain proxy. Then, service processed at a fog node moves to the final approval and validation stage. Figure 10 shows the overall process. This paper briefly explains IoT service in three stages; request, process and validation of service. If a reader wants to study further and knows details of each stage, refer to literature of blockcloud and fog computing. **(Ming et al., 2018; Atlam, Walters and Wills, 2018; Stojmenovic and Wen, 2014)**

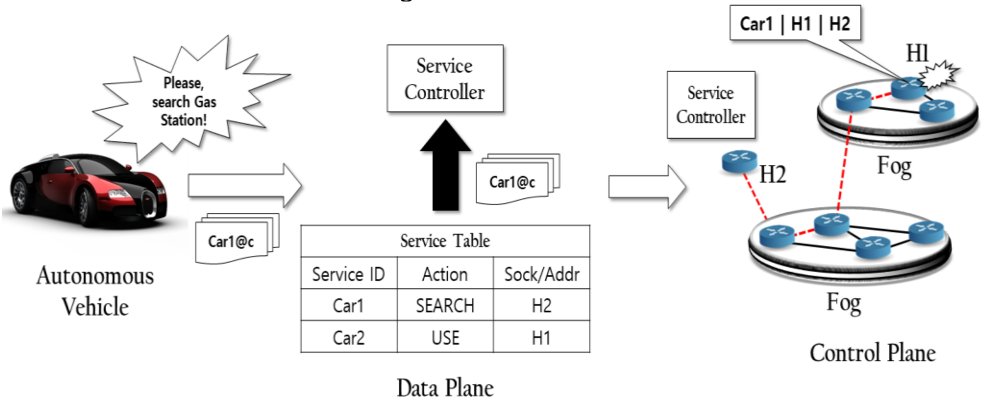
5.Service Application Model

A user is now riding an electric vehicle and notices that a vehicle's battery is going to be flat in the middle of driving. The user searches a cheap charging station among near charging stations and pay charging price to the station in advance. Then, the user visits the station and charge electricity for his vehicle, without making additional payment. The procedures are as shown in the below.

5.1.Service Transfer

To transfer a service in a SCN network, an autonomous vehicle should be allocated to a single node and request a service, In the data plane, which manages a service, a service is renewed at a service table. In the control plane, a service controller refers to service information and route to a path containing a node that can provide a service earliest.

Figure.9 SCN Network

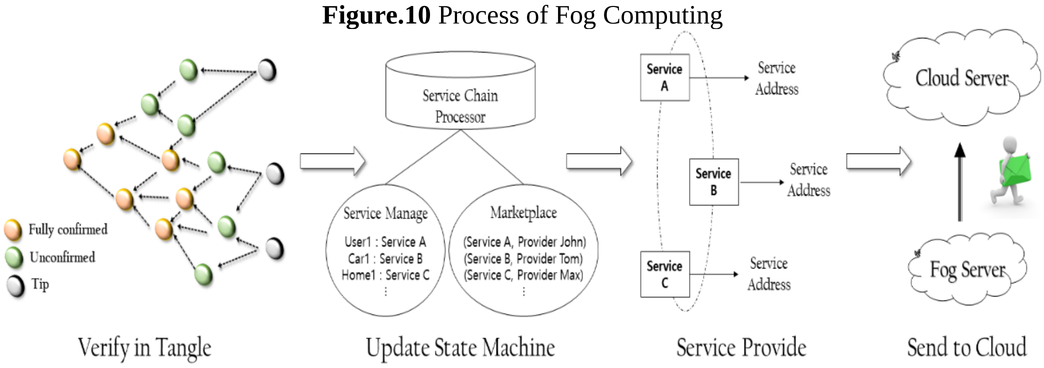


Refer to Figure 9. The service ID in the SCN network is defined as Carl before the autonomous vehicle transfers the service to a fog node in a corresponding area. The name of service to find a charging station is defined as ‘c’. The service is saved at the service table. The service path from Node H1, in which the autonomous vehicle made request for the service, to Node H2 is provided after acknowledging that the service can be provided at Node H2 in a different area through a service controller. As the system provides a service instance in a P2P form by allocating a unique number to a service job, rather than making communication with a service using an address, it can distribute duplicate service through a distributed network and route a service requested by a client to the nearest place, while maintaining the most effective network use.

5.2.Service Processing

Figure 10 shows the processing based on fog computing.

Figure.10 Process of Fog Computing

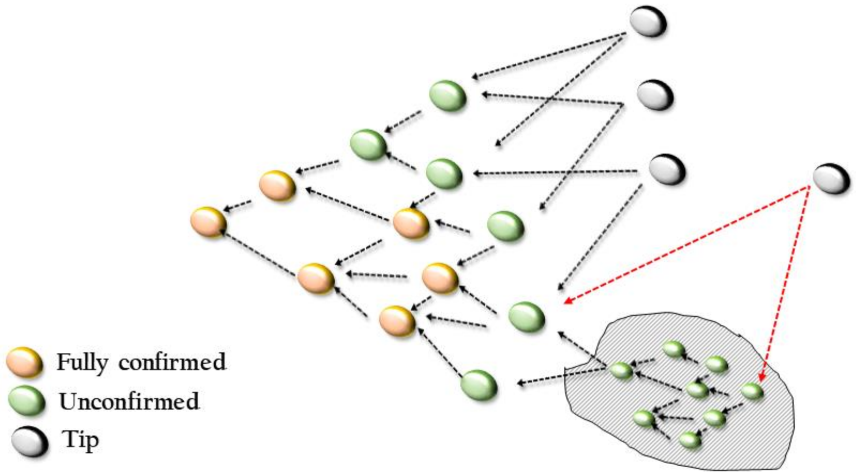


A user uses a fog proxy to access to a fog node near him/her when requesting a service. When a fog node in an area where a client belongs to is connected, a service requested by an autonomous vehicle is encoded and uploaded to a Tangle network of a fog node in a form of transaction. A transaction shall have approval of network participants. To obtain approval, two previous transactions in a Tangle structure should be approved. Once approval is obtained, modified Tangle information is recorded at a status device of a fog node through a service chain processor. Then, a service provider and price are confirmed and saved in a form of smart contract, referring to the service management table and the market place. In the inside of fog, a service based on service routing information requested by an autonomous vehicle is requested to a Tangle network as a transaction for validation and implementation. When validation is completed, electricity price is confirmed, referring to the market place. Then, a smart contract is issued, with the condition that a service user shall transfer a token to an account address of a service provider. If the contract conditions are met, a service provider provide an autonomous vehicle with a corresponding service. A user charges electricity at a station notified by the service. Then, data is processed at a fog node and service information is transferred to a cloud server.

5.3.Service Validation

Figure 11 shows the transaction verification process of the cloud server.

Figure.11 To Validate Transactions in Cloud



The final validation for service processed at a fog node is done at blockchain of a cloud server. Therefore, Tangle network information saved in a form of transaction is deleted in a certain period after the information is transferred. A server receiving information from several fog nodes verifies Tangle of a fog node as well when a new transaction validates previous transactions inside a server. It is important to note that transactions happening are invalid after a negative approval if there is negative approval given to a transaction with low trustiness among transactions validated in a fog node. Therefore, a fog node should refer to Snapshot, which contains information of overall Tangle in a cloud server, and account information, and a coordinate node in a fog node generates milestone transaction to prevent a negative transaction happening. A transaction with low trustiness shall have final approval at a cloud server.

6.Conclusion

This paper presents a new IoT model, combining characteristics of fog computing and blockchain. As the first and the second generation blockchain technology had transaction fee issues and limitations on processing speed, this study applies the third generation blockchain, IoTA, particularly, DAG based Tangle technology, which is the core technology of IoTA. However, current IoTA technology also has some issues. First, hardware design needs to be complete first. Second, there is a privacy management issue due to centralization of a certain node (coordinator). Third, there are also security issues including 34% attack. Therefore, these issues and limitation shall be dealt with before commercialization of the technology.

The possible future of IoT would be IDoT(Identity of Things) in which each device can make own decision, based on user's information. As the era of IDoT is coming, extensive studies on information security, as well as user's convenience should be conducted to ensure the era of safe and convenient.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2019R1F1A1056507).

References

A. CeArley, D., Burke, B., Searle, S., & Walker, M. J. (2016). Top 10 strategic technology trends for 2018. The Top, 10.
B. Dawson, M., Eltayeb, M., & Omar, M. (Eds.). (2016). Security solutions for hyperconnectivity and the Internet of things. IGI Global.

C. Kim, Y. (2019). Fourth Industrial Revolution (4IR) Hyper-Connected Society and Internet of Things Age. Review of Korea Contents Association, 17(3), 14-19.
D. Vermesan, O., & Friess, P. (Eds.). (2015). Building the hyperconnected society: Internet of things research and innovation value chains, ecosystems and markets (Vol. 43). River Publishers.
E. Choi, A. J. (2014, November). Internet of things: Evolution towards a hyper-connected society. In 2014 IEEE Asian Solid-State Circuits Conference (A-SSCC) (pp. 5-8). IEEE.
F. Yin, H., Guo, D., Wang, K., Jiang, Z., Lyu, Y., & Xing, J. (2018). Hyperconnected network: A decentralized trusted computing and networking paradigm. IEEE Network, 32(1), 112-117.
G. Jang, E. J., & Shin, S. J. (2020). Proposal of New Data Processing Function to Improve the Security of Self-driving Cars' Systems. The Journal of The Institute of Internet, Broadcasting and Communication, 20(4), 81-86.
H. Moon, S. H. (2020). Big Data Platform Construction and Application for Smart City Development. The Journal of the Convergence on Culture Technology, 6(2), 529-534.
I. Park, C., & Cha, J. (2019). Analysis of Component Technology for Smart City Platform. International Journal of Advanced Culture Technology, 7(3), 143-148.
J. Hwang, C., Kim, H. S., Lee, J. Y., & Jung, K. (2017). A study on BSN data collection technique through mobile devices in a cloud environment. International journal of advanced smart convergence, 6(2), 82-88.
K. Oluwatosin, H. S. (2014). Client-server model. IOSR J Comput Eng (IOSR-JCE), 16(1), 67.
L. Arsénio, A., Serra, H., Francisco, R., Nabais, F., Andrade, J., & Serrano, E. (2014). Internet of intelligent things: Bringing artificial intelligence into things and communication networks. In Inter-cooperative collective intelligence: Techniques and applications (pp. 1-37). Springer, Berlin, Heidelberg.
M. Butler, B. (2018). What is fog computing? Connecting the cloud to things. Network World.
N. Saad, M. (2018). Fog computing and its role in the internet of things: concept, security and privacy issues. Int. J. Comput. Appl, 975, 8887.
O. Jung, T. W., Lee, J. Y., & Jung, K. D. (2020). Traffic-based reinforcement learning with neural network algorithm in fog computing environment. International Journal of Internet, Broadcasting and Communication, 12(1), 144-150.
P. Griffin, D., Rio, M., Simoens, P., Smet, P., Vandeputte, F., Vermoesen, L., ... & Franke, M. (2015). Service-centric networking. In Handbook of Research on Redesigning the Future of Internet Architectures (pp. 68-95). IGI Global.
Q. Gasparyan, M., Corsini, G., Braun, T., Schiller, E., & Saltarin, J. (2017, June). Session support for SCN. In 2017 IFIP Networking Conference (IFIP Networking) and Workshops (pp. 1-6). IEEE.
R. Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Manubot.
S. Panikkar, S., Nair, S., Brody, P., & Pureswaran, V. (2015). Adept: An iot practitioner perspective. Draft Copy for Advance Review, IBM.
T. Ming, Z., Yang, S., Li, Q., Wang, D., Xu, M., Xu, K., & Cui, L. (2018). Blockcloud: A Blockchain-based service-centric network stack.
U. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.
V. Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: a review. big data and cognitive computing, 2(2), 10.
W. Stojmenovic, I., & Wen, S. (2014, September). The fog computing paradigm: Scenarios and security issues. In 2014 federated conference on computer science and information systems (pp. 1-8). IEEE.
X. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37).
Y. Buterin, V. (2018). What is Ethereum?. Ethereum Official webpage. Available: http://www. ethdocs. org/en/latest/introduction/what-is-ethereum. html. Accessed, 14.
Z. Li, Y., Cao, B., Peng, M., Zhang, L., Zhang, L., Feng, D., & Yu, J. (2019). Direct acyclic graph based blockchain for internet of things: Performance and security analysis. arXiv preprint arXiv: 1905.10925.
AA. Serguei, P. (2017). The tangle. IOTA.