Query-chain: Fast and Flexible Blockchain-based Platform for Diverse Application Services

Youhawn Seol, Jaehong Ahn, Sehyun Park,
Mookeun Ji, and Jeongyeup Paek
Chung-Ang University
Seoul, Republic of Korea
{adaan12,ahong94,po2562,wlanrms95,jpaek}@cau.ac.kr

Heungseok Chae, Jiheon Yi, Youngju Kim
ABC Inc.
Seoul, Republic of Korea
{seok,baupa,mohr}@4intel.net

***Abstract*—With increasing interest in blockchain for its immutability and decentralization, numerous blockchain-based systems and applications have been proposed, and many more attempts are underway to utilize the technology. However, several challenges such as low processing speed, scalability, and vulnerability to certain attacks have been identified, making it difficult to apply the technology on general industrial applications. In this paper, we propose a new application service platform architecture on top of blockchain that resolves those challenges. The proposed architecture takes advantage of private blockchain to secure processing speed and security while allowing public open use of the system by dividing the system into multiple layers. Assuming arbitrary nodes can participate in service, we propose periodic node verification process and '*query-chain*' to effectively authenticate and validate arbitrary nodes.**

***Index Terms*—blockchain; application platform; hierarchical architecture; decentralization;**

I. Introduction

Bitcoin, as the representative of cryptocurrency, has contributed to building a reliable decentralized cryptocurrency environment working on P2P networks without the need of central trusted authorities [1]. Blockchain is the underlying technology and data structure of Bitcoin, which contains chained blocks having a set of transactions occurred between peers. Each peer maintains a distributed ledger consisting of sequentially chained blocks which are propagated and validated by full nodes with the preset consensus protocol between validator nodes.

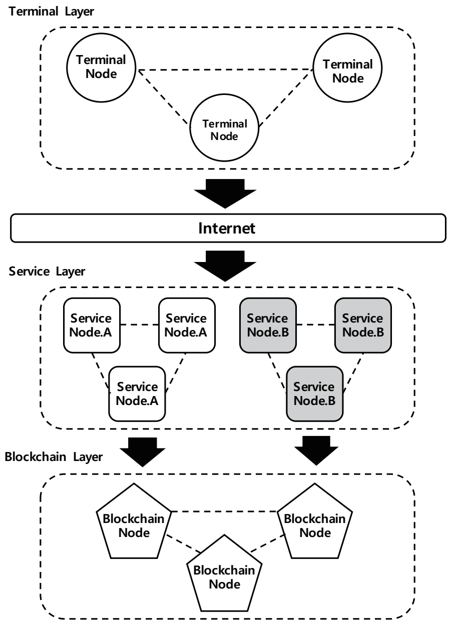

Fig. 1. Three-layered Hierarchical Architecture

In addition to being used for cryptocurrency, blockchain technology can also be utilized to ensure the reliability of data in a decentralized network where untrustworthy nodes participate and share data. That is, when an untrusted third party participates in the service operation, blockchain shows off its effectiveness, suppressing malicious users' data manipulation through the negotiation process between nodes. In various industry fields, there have been many attempts to develop variety of services based on the blockchain technology to take advantage of this property. However, the fact that a particular service prevents malicious behavior through the characteristics of blockchain implies that the server providing the services also plays a role as a full node in blockchain network [2]. As a result, service provider needs to take on handling not only business logic but also additional tasks such as maintaining blockchain and participating in mining process for verifying every block. Therefore, it is difficult to apply blockchain easily into general applications.

In this paper, we propose an application service platform structure that suppresses untrusted participants' malicious behavior by separating the service and blockchain domains while allowing the service providers to implement general business logic. In this structure, the blockchain domain and the service domain are completely separated into respective layers so that they depend only on each other's interfaces. To do so, however, it is required for the nodes which are very above

Y. Seol, S. Park, M. Ji, and J. Paek are with the School of Computer Science and Engineering, and J. Ahn is with the School of European Languages and Cultures, all at Chung-Ang University, Seoul, Republic of Korea. H. Chae, J. Yi, and Y. Kim are with the ABC Inc., Seoul, Republic of Korea. Jeongyeup Paek is the corresponding author.

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the National Program for Excellence in SW supervised by the IITP(Institute for Information & communications Technology Promotion)(20170001000031001)

978-1-7281-0893-3/19/$31.00 ©2019 IEEE

of blockchain nodes to prove their reliability and trustworthiness on their own layer. On our proposal platform structure '*query-chain*', the middle layer nodes verify each other by going through a mutual verification process. Attempting to overlay verified nodes permits blockchain nodes to remain as private. While using the 'chaining' concept of blockchain, '*query-chain*' provides a structure for service developers to develop decentralized applications without the need of deeply understanding blockchain technology. The detailed design for '*query-chain*' is covered in Section III.

II. Problem & Motivation

Blockchain has received explosive attention with the success of Bitcoin which was presented in Satoshi Nakamoto's paper [1]. Then, the birth of Ethereum [3], as the first blockchain based platform which supports smart contract, has brought the immutability and decentralization to various fields such as Internet of Things [4]–[8], Health Care [9]–[12], Digital Rights Management [13]–[15], and E-commerce [16]–[18]. However, there still exist many problems to solve for applying blockchain technology on the existing applications which are developed for server-client system in general.

First of all, it is low processing speed. Bitcoin adopted PoW (Proof-of-Work) for block consensus algorithm. This process requires enormous computing power to all of full nodes participating in blockchain network and it limits block creation cycle to 5-10 minutes on average.

The second one is limit of scalability. Basically, blockchain literally means block-chain, a set of blocks sequentially chained by the hash of previous block which also contains a set of transactions. To maintain the block-chain, a negotiation process between network participants are required. Hence, the system performance can be significantly reduced as the total network size increases. If the block size is increased to contain more transactions, the amount of information in a block can expand (thus reducing number of blocks) but the total dissemination delay including the block verification time and propagation time required for synchronizing blocks between nodes will increase [19]. This could make the blockchain network vulnerable to attacks such as double spending.

Lastly, it is a problem related to blockchain's irreversibility. Blocks recorded as agreed upon in blockchain network cannot be modified by an arbitrary user. While this property guarantees transparency of blockchain, it works against several applications that provide certain services. For instance, smart contract is automatically executed when certain preset conditions are met, and there is no way to reverse unexpected changes occurred due to malicious bugs existing in the smart contract codes.

Due to these limitations, it is still difficult to apply blockchain technology to applications, but many attempts are made to deploy blockchain based applications. In this paper, we propose the troubleshooter '*query-chain*', a platform with a new architecture that separates the service area and the data area, allowing to utilize the existing advantages of blockchain and ensure sufficient service reliability at the same time.

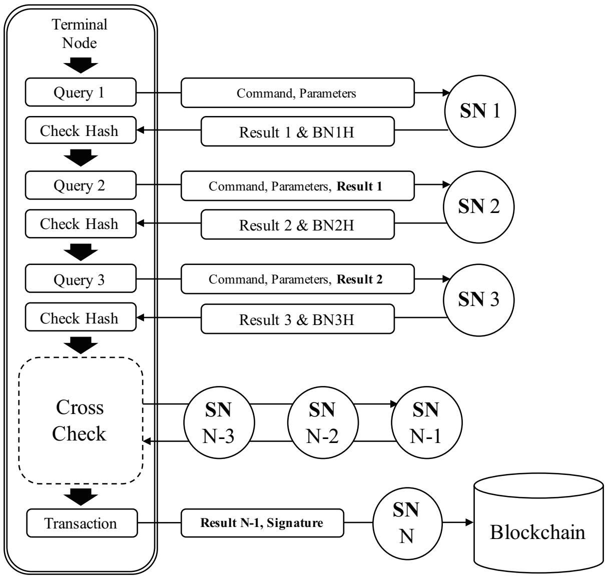

Fig. 2. Illustration of the proposed distributed logic call

III. Proposed Architecture

'*Query-chain*' maintains two separated decentralized networks, one is the 'blockchain network' that forms a distributed ledger and the other is the 'service network' that performs business logics. This allows service providers to focus on the service aspect and concern less about the blockchain part. Hence, compared to existing distributed applications that implement their services in blockchain network itself using smart contract, '*query-chain*' reduces fundamental difficulties that have to be considered.

A. Node Constitution

As shown in Fig. 1, '*query-chain*' consists of 3 parts:

Terminal Node (TN) is an endpoint user application (e.g. web app. or mobile app.) on a user side terminal that accesses the service nodes (below) to provide specific service to the users. Basically, for example, TN provides wallet management function to store address information of its user and transfer function to send certain amount of token to another user's address like typical cryptocurrencies. It also provides a function to generate transactions for particular services.

Service Node (SN) is a node where actual service designed and implemented by developers is operated and served. Service scope of SN is unlimited, and it can provide services such as smart contracts and tokens. SNs form a 'service network', which is a P2P network of its copies and seed nodes that provides list of existing SN. SNs in single domain should act like clones, and there can be multiple SN networks having different service domains.

Blockchain Node (BN) serves as a database for storing data related to the service. BN is implemented based on permissioned blockchain, so that it can provide high TPS (transactions per second) to support industrial services while

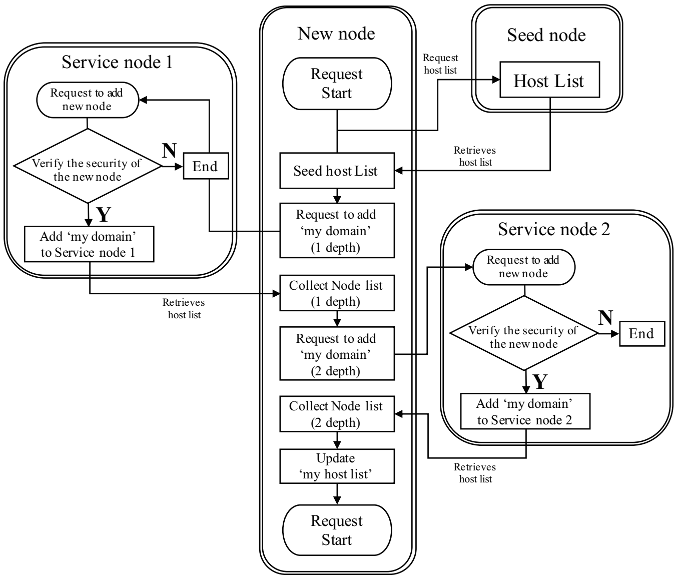
Service node 1
Request to add new node
Verify the security of the new node
N
End
Y
Add 'my domain' to Service node 1
New node
Request Start
Seed host List
Request to add 'my domain' (1 depth)
Collect Node list (1 depth)
Request to add 'my domain' (2 depth)
Collect Node list (2 depth)
Update 'my host list'
Request Start
Request host list
Seed node
Host List
Retrieves host list
Service node 2
Request to add new node
Verify the security of the new node
N
End
Y
Add 'my domain' to Service node 2
Retrieves host list
Retrieves host list

Fig. 3. Process for adding a new service node to the service network.

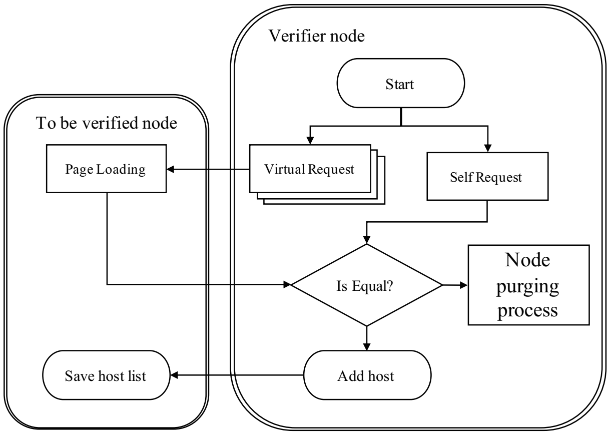

Fig. 4. Service node verification process.

maintaining characteristics of blockchain, reliability and irreversibility. Also, it is recommended to setup the BNs over VPN and using firewall so that only authorized SNs have access to the network and they are not accessible directly from the outside. This makes it possible to store service-related data more securely. Therefore, users and service providers are not required to build their own nodes to participate in the blockchain, but they only need to consider the consortium of the service networks.

B. Mechanism

In order to implement the service layer as an overlay network on permissioned blockchain network, all nodes in the service layer must be verified for their authenticity. Using the property that SNs in single domain should act like clones, several tests for authenticity can be performed.

Transaction validation process: TN generates specific transactions to use services provided by the SN. TN does not send the transaction directly to the BN, but verifies the integrity of the transaction through a distributed logic call. As shown in Fig. 2, TN divides a logic into several stages and sends queries to arbitrary SNs. The TN computes a hash (signature) for the next query using command, parameters, result, and the hash of the previous query. This makes each query form a hash chain with the previous query, and thus we call this mechanism '*query-chain*'. The same logic is executed again for a different order of arbitrary SNs from the previous one, and then TN cross-checks final signature from the first process and from the second process. Note that every SN is a clone of another and thus the final hash value must match given that there is no forgery nor malicious manipulation. After this verification, the transaction with result of the query from the (n-1)-th SN is transmitted to the n-th SN along with the signature of the user. Through the above process, it is possible to determine whether the packet is forged or not, and the integrity of the transaction can be ensured.

SN verification process Since anyone can participate in the operation of SN, there is a risk of forgery or alteration of SN. Accordingly, a verification process is essential that SN ensures the services provided by and the reliability of itself. SNs are required to be verified periodically, and new SN trying to participate in existing service network is also required to be verified as shown in Figs. 3 and 4. This verification process includes confirmation that SNs share the same domain and assurance of mutual trust. Therefore, all SNs can identify abnormal SNs or malicious SNs, remove those SNs from the network through seed nodes, and manage a blacklist to ensure reliability.

IV. Related Work

As mentioned in Section II, several limitations of blockchain still make it challenging to exploit the technology on various fields of our life. To solve those issues, many attempts were made such as the development of private and permissioned blockchain in which there exist only proven participants taking on block consensus process instead of all of full nodes participating in the network as miners. Those approaches led to reducing usage of resources and computing power consumed for the block agreement process while maintaining the structure of the hashed data chain. As one of the attempts, Linux Foundation presented HyperLedger Fabric, a platform for distributed ledger which works on the premissioned blockchain [20]. This attempt has been made to configure the permissioned blockchain network and to design the network accessible through intermediary nodes.

There have been several prior works suggesting the application of blockchain technology on various areas [4]–[18]. For example, Xia et al. presented a platform to configure access control of medical information data through blockchain [12]. It utilizes blockchain's immutability to keep track of and record every access of individuals to patients' sensitive data. In addition, the structure for blocks and transactions were newly constructed to store medical information. Schaubs et al. presented a blockchain-based trustless reputation system where every user evaluates each other after a specific transaction [21]. All of the evaluation data are safely stored in the block of which the manipulation is nearly impossible. Herbert et al. suggested a method for decentralized peer-to-peer software validation using cryptocurrency blockchain technology [22]. A user willing to get the license of a software sends a specific amount of token or money to the vendor on Bitcoin or Bespoke model.

There are many more attempts, but few were successful because blockchain-based application developers face the common problem: they need to understand how blockchain system works or build a blockchain platform which is specially designed to provide specific services. With our '*query-chain*' they can focus on implementing the service logic they want to provide to clients while utilizing all of the blockchain's properties.

V. Conclusion

In this paper, we proposed a blockchain based platform which overcomes the limitations of the existing blockchain systems and provides improved integrity and reliability. '*query-chain*' is internally composed of two separated parts: 'service network' and 'blockchain network'. This composition can reduce the possibility of data forgery in blockchain and enhance the reliability of system through self-regulating mutual verification and distributed logic call process. Furthermore, it can reduce the consensus delay of blockchain by the aid of the trust guaranteed with 'service layer'. Another advantage of layered network is that developers are not required to have deep understandings of blockchain technology to develop blockchain based services on 'terminal layer'. Similarly, the end-users do not need to maintain blockchain nodes by themselves for using the services. We anticipate invigorating various blockchain based services via our proposal platform '*query-chain*'.

As future work, we are currently in the process of implementing a large-scale industry-ready prototype of our proposed architecture, and we plan to conduct thorough performance evaluation of our system to prove its effectiveness.

References

[1] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] S. Park, S. Im, Y. Seol, and J. Paek, "Nodes in the Bitcoin Network: Comparative Measurement Study and Survey," *IEEE Access*, vol. 7, pp. 57 009–57 022, apr 2019.

[3] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[4] S.-C. Cha, T.-Y. Tsai, W.-C. Peng, T.-C. Huang, and T.-Y. Hsu, "Privacy-aware and blockchain connected gateways for users to access legacy IoT devices," in *IEEE Global Conference on Consumer Electronics (GCCE)*, 2017, pp. 1–3.

[5] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in *IEEE International Conference on Computer and Communications (ICCC)*, 2017, pp. 1180–1184.

[6] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[7] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Springer, 2017, pp. 523–533.

[8] G. C. Polyzos and N. Fotiou, "Blockchain-assisted Information Distribution for the Internet of Things," in *IEEE International Conference on Information Reuse and Integration (IRI)*, 2017, pp. 75–78.

[9] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[10] Z. Shae and J. J. Tsai, "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine," in *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2017, pp. 1972–1980.

[11] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[12] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[13] N. Fotiou and G. C. Polyzos, "Decentralized name-based security for content distribution using blockchains," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2016, pp. 415–420.

[14] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in *IEEE International Conference on Consumer Electronics-Berlin (ICCE-Berlin)*, 2015, pp. 345–346.

[15] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system," in *IEEE International Conference on Big Data and Cloud Computing (BDCloud)*, 2015, pp. 187–190.

[16] J. B. Cholewa, A. P. Shanmugam *et al.*, "Trading Real-World Assets on Blockchain-An Application of Trust-Free Transaction Systems in the Market for Lemons," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 425–440, 2017.

[17] T. Lundqvist, A. De Blanche, and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," in *Global Internet of Things Summit (GIoTS)*. IEEE, 2017, pp. 1–6.

[18] J. Ahn, M. Park, and J. Paek, "Reptor: A Model for Deriving Trust and Reputation on Blockchain-based Electronic Payment System," in *International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2018.

[19] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P Proceedings*, 2013, pp. 1–10.

[20] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018, p. 30.

[21] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2016, pp. 398–411.

[22] J. Herbert and A. Litchfield, "A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology," in *Proceedings of the 38th Australasian Computer Science Conference (ACSC)*, vol. 27, 2015, p. 30.