# A Blockchain-Based Decentralized Wi-Fi Sharing Mechanism

Yao Dai*, Zhuo Yu*, Yong Yan*, Shaoyong Guo *† and Sujie Shao *
*State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, China
†Email: syguo@bupt.edu.cn

***Abstract*—Wi-Fi is widely used as an inexpensive way for terminal service access, which brings a trend of Wi-Fi sharing. However, the current Wi-Fi sharing mode has problems such as low reliability and high cost. In order to cope with these problems, this paper puts forward a decentralized Wi-Fi sharing mechanism based on blockchain, including three sub-mechanisms of Wi-Fi authentication, Wi-Fi sharing, and Wi-Fi usage charging. Specifically, Wi-Fi owners first authenticate their Wi-Fi information on the blockchain and only the authenticated Wi-Fi can be connected. Then, the Wi-Fi users pay for the Wi-Fi usage through the smart contracts. Finally, all transactions are registered on the blockchain to ensure the security and reliability of Wi-Fi sharing process. Simulation results show that the proposed mechanism keeps a high Wi-Fi sharing success rate of more than 97 percent at a high Wi-Fi request rate of 200 tps.**

***Index Terms*—Blockchain, decentralized mechanism, Wi-Fi sharing, Wi-Fi authentication, Wi-Fi charging**

## I. Introduction

Currently, the global Wi-Fi ecosystem consists of public Wi-Fi and private Wi-Fi. Among them, public Wi-Fi is provided by Wi-Fi merchants to their users and free of use. But it's hard to realize universal coverage due to high operating costs without charging. So, more private Wi-Fi sharing should be applied to increase Wi-Fi coverage and ease of use. However, private Wi-Fi users are unwilling to provide their own Wi-Fi to unknown people if the sharing is not profitable. So some Wi-Fi sharing products appear, in which the central platform charges for Wi-Fi usage and rewards the Wi-Fi providers. But the problem regarding password leakage, information asymmetry and opaque appear in centralized operation mode for the central platform is not completely trustworthy. If the Wi-Fi sharing mechanism is decentralized, the trust can be decentralized. Therefore, there is a demand for a reliable decentralized Wi-Fi sharing mechanism. At the same time, an incentive method should be provided to encourage Wi-Fi sharing and the security of Wi-Fi sharing should also be ensured.

Motivated by the discussions above, several approaches have been proposed to provide solutions. S. Kawade et al. have proposed a paid Wi-Fi sharing mechanism to motivate private Wi-Fi sharing in [1], and K. Nakauchi et al. have provided a cloud-account-based Wi-Fi sharing method [2]. But they both adopted a centralized operation mechanism which led to information disclosure problem. To address the problem, we introduce the concept of blockchain. A blockchain is a transaction database shared by all nodes participating in a network based on a consensus protocol [3]. One key technical feature is that it enables reliable transactions without a centralized management mechanism [4] even if there are unreliable participants in the network [5]. For adopting a gossip peer-to-peer (P2P) architecture, another great technical feature is that the information of transactions can be accessed by every peer which decentralizes the credibility. These properties make the double-spending and data tampering difficult [5]. The blockchain has recently attracted the interest of stakeholders across a wide span of industries: from finance and healthcare, to utilities, real estate, and the government sector [6]. Since blockchain has great application prospects and excellent features like transparency and security [7], we apply it in the Wi-Fi sharing mechanism designing to implement secure and reliable decentralized Wi-Fi sharing.

Based on blockchain, the Wi-Fi sharing process is decentralized in which users can share Wi-Fi resources in a P2P manner. Besides, the security of the Wi-Fi sharing and charging is guaranteed by recording transactions on the blockchain. In more detail, all kinds of Wi-Fi are encouraged to share for compatibility firstly. Secondly, Wi-Fi is directly shared among users in a P2P sharing network based on smart contract [8], [9], the sharing system does not handle the keys to avoid key leaking. Thirdly, to inspire more Wi-Fi sharing, the Wi-Fi users reward the providers. Finally, the transactions generated by P2P applications will be packaged to form new blocks [10], thereby ensuring the transactions not be tampered with even if there is no centralized platform with special privileges. Although block generation may introduce some delay, the experimental results in section V indicate that it can achieve reliability with a tolerable delay. The main contributions of the research are summarized as follows.

- This paper proposes a decentralized Wi-Fi sharing mechanism based on blockchain technology, which can guarantee the security and reliability of Wi-Fi sharing.
- We also propose to perform Wi-Fi charging transactions for non-free Wi-Fis based on smart contracts to encourage more Wi-Fi sharing while guaranteeing safety.

This paper is organized as follows: Section II reviews the related work and discusses the use of blockchain in Wi-Fi sharing. Section III presents the system model and section

978-3-903176-15-7 

IV details the design and implementation of the proposed blockchain-based Wi-Fi sharing mechanism. The evaluation results are presented in Section V, followed by the conclusions in Section VI.

## II. Related Work

Current Wi-Fi sharing mechanism faces problems like low utilization, different Wi-Fi incompatibility, high cost and insecure Wi-Fi sharing, which has interested the researchers recently. Several approaches have been proposed to provide solutions.

L. Navarro et al. discussed the technological opportunities of combining blockchain with Wi-Fi networks, the options for pricing and investment models in [11]. Blockchains with digital identities, claims, tokens and smart contracts enables crowdfunding investment campaigns or direct peer transfers [11]. What's more, decentralised networking combined with financial technologies allows building self-sustaining crowdsourced infrastructures [11]. In terms of organisational and economic models, complementary perspectives were took into consideration from the different alternative.

P. Antoniadis et al. proposed that blockchain could be the underlying implementation solution for any alternative currency in [12]. Then they advanced the work by exploring two different ways through which an alternative currency model could support an existing Community Network. Since blockchains entail certain important threats, they discussed separately recent blockchain solutions that are part of the global cryptocurrency ecosystem.

[13] presented a model to enhance a specific collaborative wireless sharing service. In order to exclude malicious users, they used the SECURE model [13] for the collaborative Wi-Fi sharing service. An appropriate cooperation incentive schema was adopted to provide enough incentives for Wi-Fi sharing. But it did not break the existing centralized Wi-Fi sharing mechanism.

Motivated by existing researches, we integrate the league blockchain into the design of the decentralized Wi-Fi sharing mechanism. The blockchain works on authenticating the Wi-Fi sharing and charging transactions to ensure system reliability and security.

## III. System model

Based on the analysis presented in the previous sections, blockchain is introduced to provide a trusted environment for Wi-Fi sharing. As shown in Fig. 1, there are three roles in the network, the blockchain-based Wi-Fi sharing server, the Wi-Fi sharer, and the Wi-Fi user. The Wi-Fi sharer is more specifically divided into the public Wi-Fi sharer and the private Wi-Fi sharer. Among them, public Wi-Fi can set the charging rules as free, it is only propagated by the blockchain to be visible to more users. Private Wi-Fi profits from charging for others' Wi-Fi usage via the blockchain. In addition, the corresponding functions of the blockchain-based Wi-Fi sharing server are realized by designing smart contracts.

In the Wi-Fi sharing process, Wi-Fi sharers register their Wi-Fi information on the blockchain while providing Wi-Fi resources, which will trigger the registration smart contract to verify the sharers' account information and the Wi-Fi information. Then, the verified Wi-Fi information is registered on the blockchain and the registration result is returned to the sharer. All the Wi-Fi resources registered on the blockchain are available to users. When there is a need for accessing into Wi-Fi, the user sends the Wi-Fi connection request to the blockchain including its favorite Wi-Fi's SSID. Then, Wi-Fi connection management smart contract is responsible for establishing a P2P connection for the Wi-Fi sharer and the user to exchange keys, it just monitors the key exchanging process but does not handle the key. In order to reward reliable providers with Wi-Fi resources [14], the Wi-Fi usage is charged by charging smart contracts. Finally, transactions are recorded in the blockchain which also contributes to credibility [14]. The specific function implementation and smart contract implementation will be introduced in the next section.

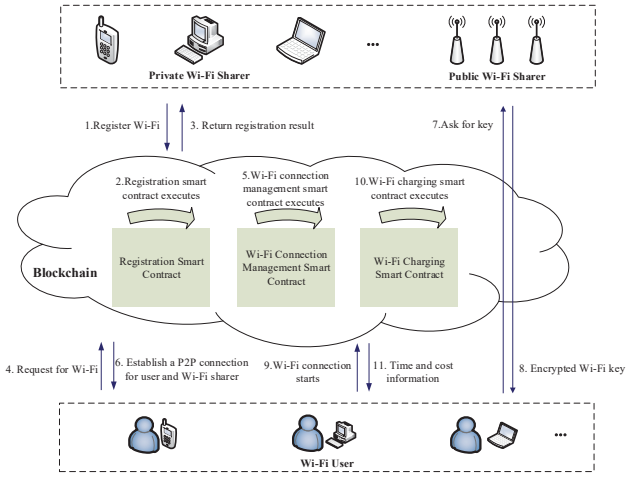


Fig. 1. Wi-Fi sharing based on blockchain.

## IV. System Design and Implementation

In this section, we will introduce the system design and implementation by specifying the system function modules and system business processes.

### A. System Function Module

Fig. 2 presents the architecture of the proposed model, which is categorized into the blockchain-based Wi-Fi sharing server, the Wi-Fi sharing terminal, and the Wi-Fi using terminal. The blockchain-based Wi-Fi sharing server acts as an intermediary to authenticate the Wi-Fi sharers and the Wi-Fi users. It propagates Wi-Fi resources from Wi-Fi sharers to Wi-Fi users and charges for Wi-Fi usage according to the rules set by Wi-Fi sharers. Next, we design functional modules to realize functions of the three entities.

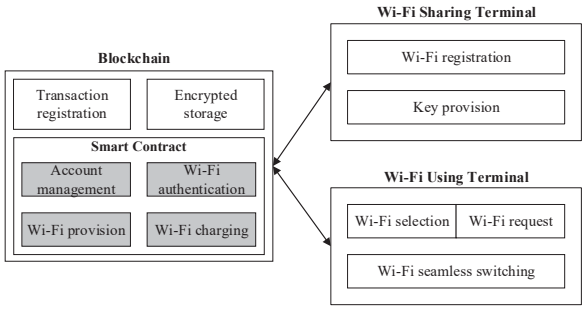


Fig. 2. System function module division.

*1) Blockchain-based Wi-Fi Sharing Server:* The server can be subdivided into six modules as Fig. 2. Among them, account management, Wi-Fi authentication, Wi-Fi provision and Wi-Fi charging module are implemented by designing smart contracts. And transaction registration and encrypted storage module are guaranteed by the nature of the blockchain. The function of each module is detailed below.

- Account management: This module manages and verifies account information. The account information includes the account ID and the account key which will be verified at the subsequent login, and the balance which is initially set to be 0.
- Wi-Fi authentication: This module is responsible for interacting with the Wi-Fi sharing terminal to register Wi-Fi information on the blockchain. After receiving the Wi-Fi registration request from the Wi-Fi sharer, the Wi-Fi information is first authenticated and then registered on the blockchain in encrypted storage.
- Wi-Fi provision: When receiving the Wi-Fi connection request from the Wi-Fi user, this module establishes a connection for the Wi-Fi user and the Wi-Fi sharer instead of participating in key sharing. It issues a signature to the Wi-Fi user which is used for the Wi-Fi sharer to verify the identity of the Wi-Fi user. Only if the signature is verified can the sharer provide the key.
- Wi-Fi charging: The payment module monitors users' Wi-Fi using time, and then the corresponding cost is deducted from the Wi-Fi user's account and transferred to the Wi-Fi sharer's account.
- Transaction registration: Wi-Fi registration, charging transactions as mentioned above are broadcast to consensus nodes by the blockchain. After the consistency algorithm processing, the transaction becomes a valid one and a new block is generated to confirm the transaction.
- Encrypted storage: The Wi-Fi information and transaction data on the blockchain are encrypted by asymmetric encryption, and only certain users with the private key can access specific data.

*2) Wi-Fi Sharing Terminal:* The Wi-Fi sharing terminal is the private mobile device or public base station which provides available Wi-Fi. We divide the Wi-Fi sharing terminal into Wi-Fi registration module and key provision module, which are introduced below.

- Wi-Fi registration: When a Wi-Fi is first shared, this module actively registers the Wi-Fi information on the blockchain by sending a registration request including Wi-Fi IP address, MAC address, SSID, network speed, Wi-Fi GPS and charging rule.
- Key provision: This module monitors connection requests from peer nodes in real time. After receiving the Wi-Fi connection request, this module verifies the requester's signature to ensure that the requester is authenticated by the blockchain. Then the Wi-Fi key is given to the requester with valid signature in encrypted form. This means that the blockchain only supervises key exchange transactions but does not participate in key processing or transmission, thus ensuring that only Wi-Fi sharers have privacy and management rights to their own Wi-Fi.

*3) Wi-Fi Using Terminal:* Wi-Fi users access into Wi-Fi through the Wi-Fi using terminal. For ease of use, Wi-Fi selection, Wi-Fi request, and Wi-Fi seamless switching module are designed for the Wi-Fi using terminal as follows.

- Wi-Fi selection: The Wi-Fi selection module selects a suitable Wi-Fi from the available Wi-Fi list according to the user preference. Users set preferences before logging in to the client, which is, strong-signal-Wi-Fi preferred or free Wi-Fi preferred.
- Wi-Fi request: This module connects to the Wi-Fi selection module. After selecting a Wi-Fi, the Wi-Fi user establishes connection with the Wi-Fi sharer to request the Wi-Fi key. After the Wi-Fi sharer verifies the Wi-Fi user's identity, the Wi-Fi key is encrypted by the public key and sent to the Wi-Fi user. At last, the Wi-Fi user decrypts the Wi-Fi key with his private key.
- Wi-Fi seamless switching: If the user terminal switches between different APs during the move, it needs to constantly log in to connect to Wi-Fi. In order to avoid this trouble, this module monitors the surrounding Wi-Fi status in real time, and once the current Wi-Fi signal is weakened, it notices the blockchain to get another Wi-Fi information, thereby seamlessly switching to another Wi-Fi.

### *B. System Business Process*

Understanding the system function modules, the specific workflow will be explained in this section. Two main events in the system are Wi-Fi registration and Wi-Fi connection.

*1) Wi-Fi registration:* Wi-Fi registration workflow is displayed in Fig. 3 and the details are as follows.

- First, the Wi-Fi sharer logs in to the system via the account ID and account password. After logging in, it sets its charging rule to free or for a charge.
- Then the encrypted Wi-Fi information is sent to the server to initiate a Wi-Fi registration request.
- After receiving a Wi-Fi registration request, the blockchain authenticates the Wi-Fi resource by verifying its security. Once the authentication is passed, it will be registered as a digital asset by multiple block nodes on the blockchain.

- Finally, the registration transaction is broadcast to the blockchain network for consensus. If the registration transaction passes the consensus process, it will be recorded in a new block. Then the blockchain returns the Wi-Fi registration result.

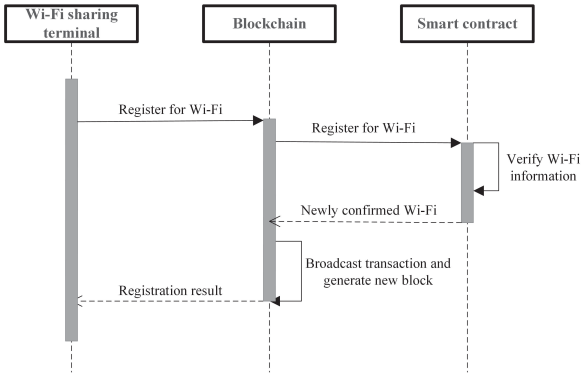


Fig. 3. Wi-Fi registration workflow.

*2) Wi-Fi connection:* Fig. 4 presents the Wi-Fi connection workflow, and the specific workflow is presented below.

- Wi-Fi request: The Wi-Fi using terminal selects the most suitable Wi-Fi according to the user preference and transmits the Wi-Fi connection request to the blockchain.
- Wi-Fi providing: After accepting a new Wi-Fi request from the user, the blockchain sends the Wi-Fi information to the Wi-Fi using terminal. The information is locally formed into a Wi-Fi list according to the signal strength.
- Wi-Fi connection: Then the smart contract is called to issue a signature to the Wi-Fi user and establish a P2P connection between the Wi-Fi sharing terminal and the Wi-Fi using terminal for key exchanging. In order to verify the Wi-Fi user's identity, the Wi-Fi sharing terminal verifies the signature. If the verification is passed, the key is provided in encrypted form.
- Wi-Fi usage charging: Once the Wi-Fi is successfully connected, the charging smart contract on the blockchain begins to execute so that the Wi-Fi using terminal automatically pays to the Wi-Fi sharers.
- Transaction certification: Blockchain broadcasts all the transactions to other nodes. The nodes accepting the transaction on the entire network execute the consensus algorithm on the block. After passing the consensus algorithm processing, the transaction becomes a valid transaction and a new block is generated to confirm the transaction.

## V. Experimental Results And Evaluation

Experimentally, so far, we implement the blockchain-based Wi-Fi sharing system using Hyperledger Fabric [15] to write smart contracts on the blockchain. It is an implementation of a distributed ledger platform for running smart contracts. Leveraging familiar and proven technologies, it allows pluggable implementations of various functions with a modular architecture

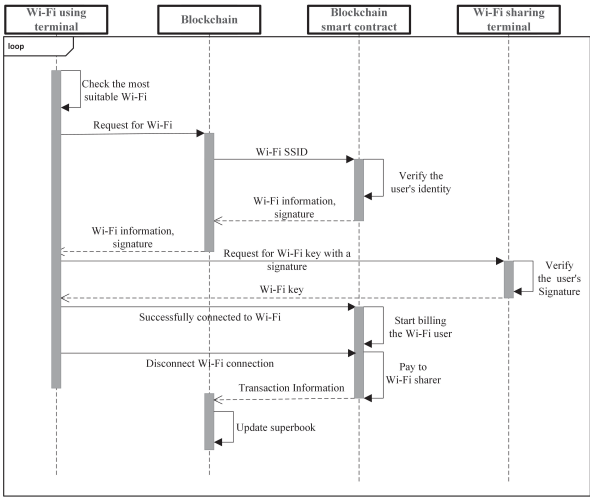


Fig. 4. Wi-Fi connection workflow.

[16]. The Fabric network is divided into four organizations, each enables two peers. Each peer is installed on a x64 virtual machine with 32 vCPUs. The PBFT [17]consensus algorithm which is a classic distributed consensus algorithm that requires at least 4 processing nodes is used for consensus.

### A. Experimental Results

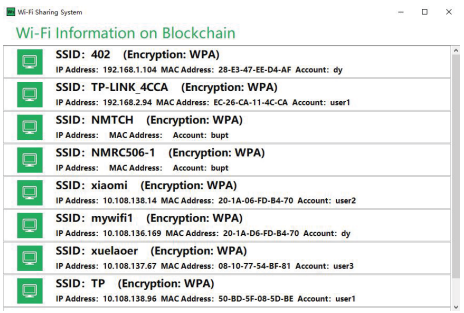


Fig. 5. Blockchain-based Wi-Fi sharing server demo.

For testing, we register some Wi-Fi information on the blockchain. So through the server interface we can see all registered Wi-Fi information arranged by registration time on the blockchain as Fig. 5.

Users with Wi-Fi using clients can access to Wi-Fi. As shown in Fig. 6, the client presents the user with a list of available Wi-Fi information, and automatically selects the strongest Wi-Fi named 402 for the user.

User account balance information are arranged by registration time as shown in Fig. 7. We choose dy and user2 account to test, whose original balance are 10 and 40, as shown in Fig. 7(a). If the charging rule of dy is 1 token per minute, after user2 connects to 402 whose account is dy for ten minutes, its balance reduces to 30 while the dy user's balance increases to 20 as Fig. 7(b). The experimental results show that the system performs correctly.

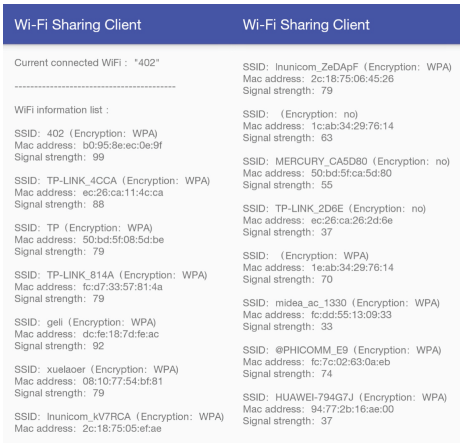


Fig. 6. Wi-Fi sharing client demo.

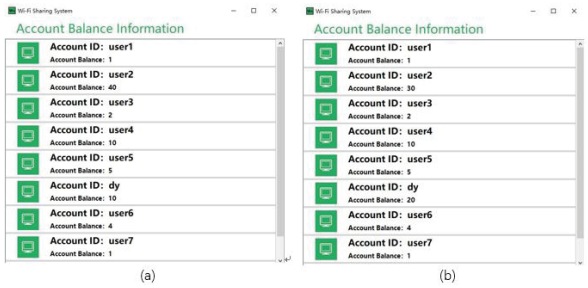


Fig. 7. Account information on blockchain.

## B. System Evaluation

The system performance is measured by throughput, delay, and success rate. Among them, throughput is the number of transactions submitted to the ledger per second(tps), delay is the blockchain response time, and success rate is the Wi-Fi connection success rate.

We consider some parameters that have an impact on the Wi-Fi connection service, such as the number of vCPUs occupied by the server, the number of Fabric channels, and the Wi-Fi request service arrival rate. Note that a channel is a ”private” subnet of communication between several peers in a Fabric [17]. Transactions on a Fabric channel are only seen by peers and participants. Therefore, the channel implements a degree of parallelism for transactions in Fabric. In our experiment, the number of channels defaults to 4 and the vCPU number defaults to 16. Next, we will discuss the effect of each parameter on the system performance.

The relationship between request arrival rate and average success rate is shown in Fig. 8. When the Wi-Fi request arrival rate increases, the average success rate drops slightly. This is because a Wi-Fi request contains multiple invoke and query operations. High concurrency may bring a slight error rate, but no more than 5 thousandths. In addition, Fabric with 8 channels has a higher average success rate than 4 and 2 channels, indicating that multiple channels improves system concurrency.

Fig. 9. compares the average success rate for different vCPU numbers with request arrival rates of 100 tps, 120 tps and 140

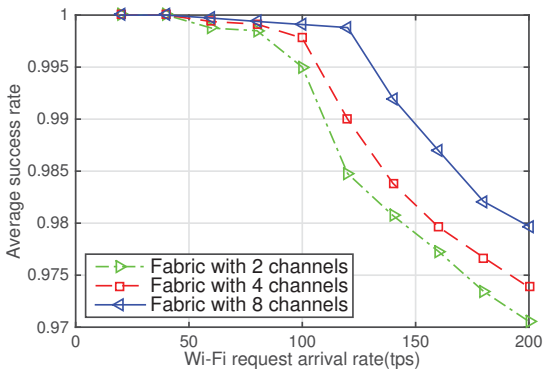


Fig. 8. Wi-Fi request arrival rate and the average success rate of Wi-Fi requests.

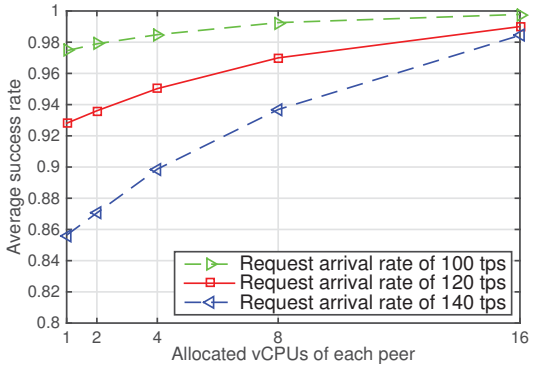


Fig. 9. Number of allocated vCPUs and the average success rate of Wi-Fi requests.

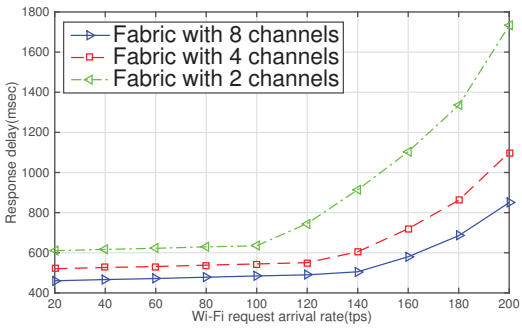


Fig. 10. Wi-Fi request arrival rate and the response delay.

tps. As the number of vCPUs occupied by nodes increases, the system achieves a higher average success rate. When the number of vCPUs is less than the number of channels and the service arrival rate reaches the saturation point, the average success rate is slightly lower. For example, in the case of one vCPU allocated, the average success rate is only 85.5 percent. Therefore, realizing parallelism by assigning at least one vCPU to each channel ensures higher quality of service.

In Fig. 10, when the arrival rate is below the saturation point, as the arrival rate increases, the delay increases slightly. But when the arrival rate is near or above the saturation point, the delay increases significantly as the Wi-Fi arrival

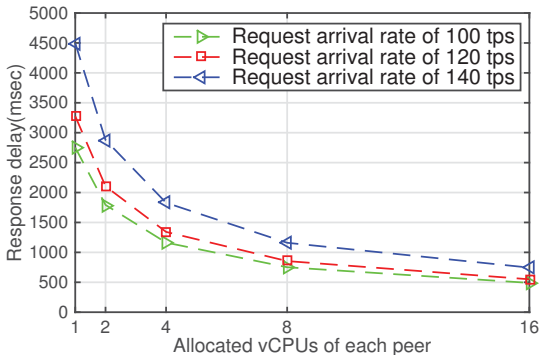


Fig. 11. Number of allocated vCPUs and the response delay.

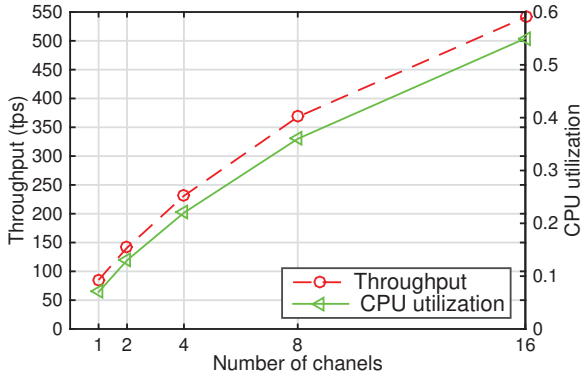


Fig. 12. Number of channels, the throughput and the CPU utilization.

rate increases. This is reasonable because the transactions wait longer in the waiting queue. What's more, the fewer the number of channels, the faster the transaction processing volume reaches the saturation point. Fabric with 8 channels arrives at the saturation point at 140 tps while Fabric with 2 channels reaches the saturation point at only 100 tps. So it is recommended to open multiple channels to increase parallel processing to reduce latency.

Considering the effect of vCPUs, Fig. 11. compares the relationship between response delay and vCPU number. When there are only one vCPU, the processing delay even exceeds 4500 milliseconds. With an increase in vCPU number, the service delay decreases as expected. Due to that the more vCPUs, the higher the ability to process transactions in parallel. Since each channel can get more vCPUs, it is faster to perform verification transactions and submit ledgers, thus reducing response delays observably.

Fig. 12. displays that with an increase in channel number, both CPU utilization and throughput increase. In the multiple channels case, each channel processes a portion of the block generation transactions, so the verification phase and final ledger update of multiple blocks executed in parallel increases CPU utilization, resulting in higher throughput.

## VI. Conclusion

In this paper, considering of the reliability, security and utilization problem of traditional Wi-Fi sharing mode, we integrate blockchain into the design of the decentralized Wi-Fi sharing mechanism. Specifically, blockchain authenticates the Wi-Fi resources and charges for Wi-Fi usage to provide trusted service without a trusted intermediary. Registering all transactions on the blockchain also contributes to system security and reliability. Finally, we implement the proposed mechanism on the Hyperledger Fabric, and the simulation results show that the system performs well.

## Acknowledgment

This work is jointly supported by National Natural Science Foundation of China (Grant.61702048) and Science and Technology Project from Headquarters of State Grid Corporation of China: "Key technology development and application demonstration of high-confidence intelligent sensing and interactive integrated service system(No.52110418002V)".

## References

[1] S. Kawade, J. . V. Bloem, V. S. Abhayawardhana, and D. Wisely, "Sharing your urban residential wifi (ur-wifi)," in *2006 IEEE 63rd Vehicular Technology Conference*, vol. 1, May 2006, pp. 162–166.

[2] K. Nakauchi and N. Nishinaga, "Software-defined exchange for the virtualized wifi network towards future mobile cloud services," in *2016 IEEE International Conference on Communications Workshops (ICC)*, May 2016, pp. 736–741.

[3] M. Samaniego and R. Deters, "Blockchain as a service for iot," pp. 433–436, Dec 2016.

[4] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. O'Reilly Media, Inc., 2015.

[5] X. Min, Q. Li, L. Liu, and L. Cui, "A permissioned blockchain framework for supporting instant transaction and dynamic block size," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug 2016, pp. 90–96.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[7] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[8] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *2016 IEEE International Conference on Consumer Electronics (ICCE)*, Jan 2016, pp. 467–468.

[9] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain," in *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)*, Oct 2015, pp. 577–578.

[10] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed p2p applications," *IEEE Access*, vol. 6, pp. 27 324–27 335, 2018.

[11] L. Navarro, I. Castro, A. Sathiaseelan, E. Dimogerontakis, M. Selimi, and R. Baig, "Blockchain models for universal connectivity."

[12] P. Antoniadis and J. Martignoni, "What could blockchain do for community networks."

[13] C. B. Lafuente and J. Seigneur, "Achieving collaborative wi-fi sharing without changing current technologies," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, July 2013, pp. 1510–1515.

[14] P. K. Sharma, M. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[15] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, and Y. Manevich, "Hyperledger fabric: A distributed operating system for permissioned blockchains," 2018.

[16] A. Stanciu, "Blockchain based distributed control system for edge computing," in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, May 2017, pp. 667–671.

[17] H. Sukhwani, J. M. Martnez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric)," in *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, Sept 2017, pp. 253–255.