

# Blockchain as a Platform for Secure Cloud Computing Services

Wang-You Tsai\*, Tzu-Chuan Chou\*, Jiann-Liang Chen\*\*, Yi-Wei Ma\*\* and Chen-Jui Huang\*\*

\*Department of Information Management, National Taiwan University of Science and Technology, Taiwan

\*\*Department of Electrical Engineering, National Taiwan University of Science and Technology, Taiwan

**Abstract**— Problems related to privacy and cyber-attacks have increased in recent years as a result of the rapid development of cloud computing. This work concerns secure cloud computing services on a blockchain platform, called cloud@blockchain, which benefit from the anonymity and immutability of blockchain. Two functions- anonymous file sharing and inspections to find illegally uploaded files- on cloud@blockchain are designed. On cloud@blockchain, cloud users can access data through smart contracts, and recognize all users within the application layer. The performance of three architectures- a pure blockchain, a hybrid blockchain with cache and a traditional database in accessing data is analyzed. The results reveal the superiority of the hybrid blockchain with the cache over the pure blockchain and the traditional database, which it outperforms by 500% and 53.19%, respectively.

**Keywords**— Blockchain as a Platform, Secure Cloud Computing, Cyber-Attack, Privacy, Smart Contract

## I. INTRODUCTION

With the rapid development of communication and computing technology, various cloud applications have been developed. Most services like Google Drive, Dropbox or Mega are based on centralized architecture, but the unreliability of centralized applications is evident. In one of the most famous relevant cases, Facebook had failed to protect the privacy of its users, allowing the British Cambridge Analysis company to obtain a large amount of user data, allegedly with the goal of influencing elections in the US. Two years ago, Taiwan's First Bank was the victim an ATM heist after a Trojan was into the host in the bank's London branch. These two cases reveal that services that are controlled by a single organization are vulnerable to human error and bugs in the system, which can result in the loss of personal property. To improve data privacy, the EU passed the General Data Protection Regulation (GDPR), which is the most far-reaching bill on data privacy to date.

How can vulnerability to attacks be reduced, the right to use data maintained, and the advantages of original services maintained? In this work, a secure cloud computing architecture that is based on blockchain technology, called cloud@blockchain, is designed. In cloud@blockchain, each node has a public transaction book. All transactions are recorded and anyone can confirm their integrity and legitimacy [1]. A decentralized application on cloud@blockchain is designed to prevent file infringement, protecting privacy. The proposed cloud@blockchain can be

used in many scenarios, including anonymous contest and digital certificate verification [2,3].

In this study, two mechanisms that operate on cloud@blockchain are developed to improve upon existing cloud computing services.

A. Anonymous file sharing: The cloud storage service collects a large amount of user data. The anonymous file sharing mechanism on cloud@blockchain allows users to share files with their privacy protected.

B. Inspection for illegally uploaded files: A unique fingerprint is generated and uploaded to the blockchain for storage. Whenever a file is uploaded, whether the file uploader is the owner can be easily determined [4].

The rest of this paper is organized as follows. Section 2 provides a brief background on blockchain architecture and the state of art. Section 3 presents blockchain-based approaches to providing secure cloud computing. Section 4 analyzes the performance of traditional and blockchain-based approaches to file sharing and inspection. Finally, Section 5 summarizes the discussion and emphasizes the main points.

## II. RELATED WORKS

The blockchain was conceptualized and developed by Satoshi Nakamoto [5]. Based on blockchain computing, all transactions are recorded and can be verified by anyone. Since the computations involve one-way hash functions, the nodes in the blockchain can rapidly identify which chain is correct. Many blockchain computing technologies have been developed, including Ethereum, Iota and Zcash. They use different consensus and encryption mechanisms to derive various forms of computing, functionality and security. Figure 1 presents blockchain computing [6-8].

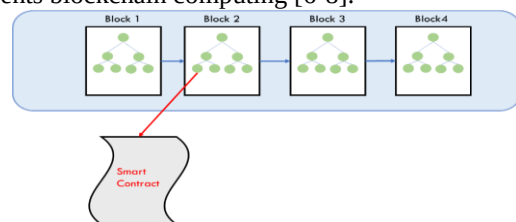


Figure 1. Blockchain Computing

One of the most important technical contributions of blockchain computing is the smart contract [9]. Smart contracts are programs that are stored on the blockchain and assist in the verification and execution of contracts. In the

Ethereum system, users on the local side can execute contract functions using `eth.call` and `eth.sendTransaction`. A contract is executed on the Ethereum Virtual Machine (EVM). All executions are inseparable from the EVM. Practically, the EVM can be considered to be a large distributed computer. Figure 2 presents the contract process in the Ethereum system.

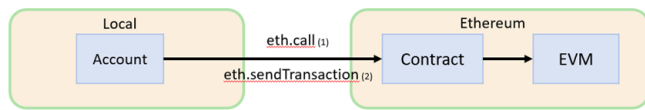


Figure 2. Smart contract process in the Ethereum system

Many works have sought to improve the security and privacy of cloud computing using the blockchain [10-12]. References [12] and [13] defined and introduced the base technology of the blockchain and reviewed previous studies considering cloud computing environments. In the ProvChain architecture, a provenance auditor is used to manage a cloud service provider and access to the blockchain [14]. In the anonymous Wi-Fi hotspot architecture, the server of the service provider is used to update the checkpoint data in the blockchain [15].

### III. PROPOSED CLOUD@BLOCKCHAIN ARCHITECTURE AND OPERATIONS PROBLEM SOLUTION

Figure 3 shows general cloud computing architecture. User data are protected against unauthorized access by account-based security procedures. The blockchain-based cloud computing differs from traditional computing in many application scenarios and many aspects of data transactions. Figure 4 presents the proposed cloud@blockchain architecture, which comprises Blockchain, Smart Contract, Cloud Storage and file owner. The overall system consists of the operating system, a fully functional application and a signal function unit. This system has a flat design and all applications are based on the blockchain platform, so all applications in this study are called “user”. Smart Contract is the mediation layer that is used for communication. Smart Contract can process and store metadata that are uploaded by owner. On the user side, any cryptographic algorithm, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), can be used to confirm quickly the identity of the data owner. Users (cloud side) can provide online storage services, having received an upload request from the owner (user side). The cloud storage facility can verify the owner's permission through the authentication unit, the upload unit, the file storage unit and the mapper. The blockchain preserves the anonymity of owners while remaining open to public inspection. Although nothing is totally secure, tampering with blockchain is almost impossible.

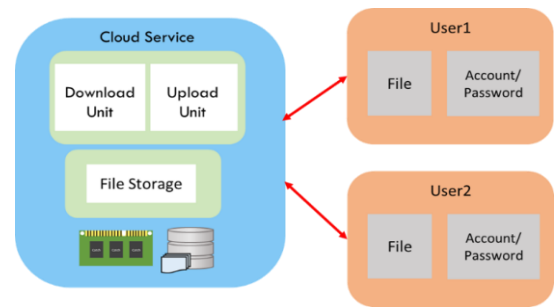


Figure 3. The general cloud computing architecture

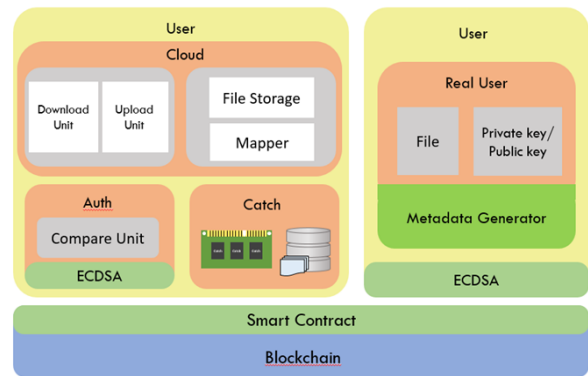


Figure 4. The proposed cloud@blockchain architecture

#### A. Anonymous file sharing mechanism

A traditional Decentralized application (Dapp) architecture, in which all operations are controlled by a centralized service. Even when the user wants to do something that has nothing to do with other users, it must pass through a centralized service. The proposed framework, each user can see that no one can hold all of the operation rights. For example, a cloud service provider only be responsible for part of a service, and then the writing and correctness of the information give back to the owner to dealing. Decentralized architecture clearly defines and minimizes the power of each person.

##### 1) Uploading on cloud@blockchain

Figure 5 presents the process of uploading on cloud@blockchain. The steps include updating file information (Metadata) to the blockchain; uploading a file to a cloud storage node; reading data from the blockchain, and comparing the file's hash, respectively. Finally, the read/write procedure is performed.

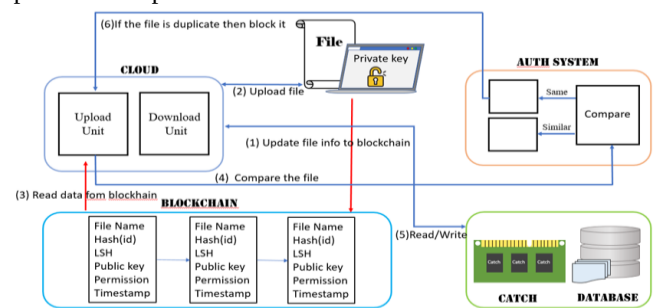


Figure 5. Uploading on cloud@blockchain

## 2) Downloading on cloud@blockchain

Figure 6 presents the process of downloading on cloud@blockchain. After it has been uploaded, a data file can be downloaded. The first step is to read the metadata in the blockchain. The cloud storage node then uses SimHash for similarity comparison. The user can determine from the address whether the most similar file matches the original file. Finally, the user can decide whether to download the file.

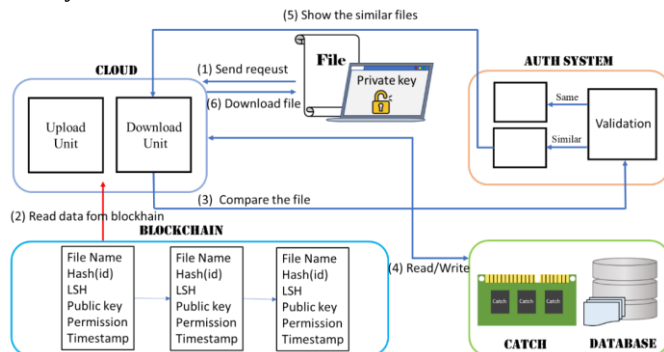


Figure 6. Downloading on cloud@blockchain

### B. Inspection for illegally uploaded files on cloud@blockchain

The process of uploading mainly provides storage space and what to do with user authority determination result. Here, hash ID verification and signature authentication are used in the uploading process to confirm the user. Blockchain computing allows the authentication system to operate independently of the cloud, and ensures the independence of the authentication. Figure 7 shows the steps in inspecting a file.

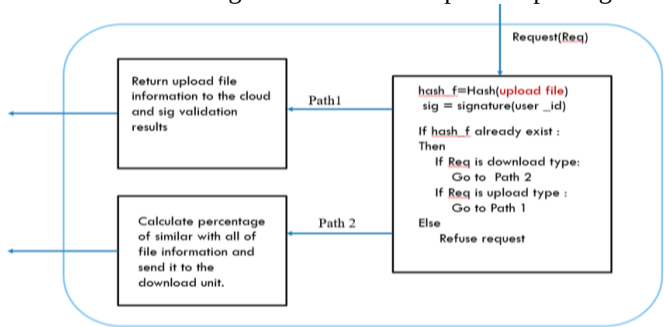


Figure 7. Inspection steps

## IV. PERFORMANCE ANALYSIS

To determine the feasibility of the proposed cloud@blockchain, a trial is performed using the Ethereum Wallet Backend, which involves the functions of sendTransaction, call method, lookup accounts, and sign. The mediation layer, Smart Contract, is written by Solidity and deployed to the EVM.

Figure 8 presents the simulation parameters herein. This parameter is used to generate the Genesis Block. The higher the difficulty is, the safer it is. If the available computing resources are not enough, then the transaction speed may be lower. The gasLimit is the set upper limit on the execution time to prevent all loops from consuming all EVM resources.

```
"nonce": "0x00000000000000000000000000000000",
"difficulty": "0x020000",
"mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000",
"coinbase": "0x0000000000000000000000000000000000000000000000000000000000000000",
"timestamp": "0x00",
"parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
"extraData": "0x11bbe8db4e347b448c937c1e8370e4b5ed33adb3db69cbbdb7a38e1e50b1b82fa",
"gasLimit": "0x4c4b40"
```

Figure 8. Simulation parameters

Based on the above description, storing data in a Smart Contract consumes gas, which is converted from ether. An interface is designed to facilitate the sending of a transaction by a user. After a transaction is sent through the user interface, the node decides which transaction to handle first; it usually selected the one that involves the highest price first.

Figure 9, Fig. 10, Fig. 11 and Table 1 present the results of performance analyses of a pure blockchain (Method 1), a hybrid blockchain with cache (Method 2) and a traditional database (Method 3).

| Requests<br>Label | #Samples | Executions |         | Response<br>Times (ms) | Throughput<br>(req/sec) | Network (KB/sec) |       |
|-------------------|----------|------------|---------|------------------------|-------------------------|------------------|-------|
|                   |          | KO         | Error % |                        |                         | Received         | Sent  |
| Total             | 60000    | 0          | 0.00%   | 69.1                   | 95.31                   | 244.78           | 18.99 |

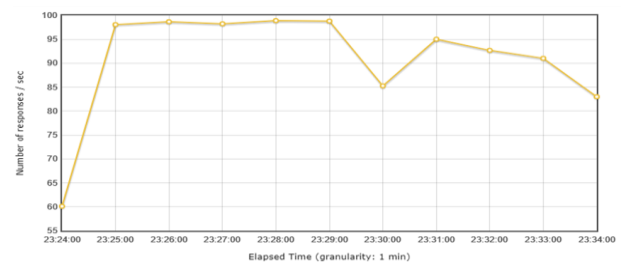


Figure 9. Performance analysis of Method 3

Figure 9 shows the average performance for a total of 60000 requests (0 error) by using Method 3. In the process of uploading, the average response times is 69.1ms and the throughput is 95.31 req/s. Figure 10 shows the average throughput of the three methods. Cloud@blockchain can provide a throughput of nearly 15 req/s (around 9000 requests in 10 minutes); cloud@blockchain with cache reaches 90 req/s or more. (about 60,000 requests in 10 minutes, Figure 9); and the traditional database can achieve 170 req/s or more (about 100,000 requests in 10 minutes). From Figure 10, the performance without a cache is not good. The cache improves performance by about six times. The cache reduced the gap between the cloud@blockchain solution and traditional database solution to a factor of 1.88 times.

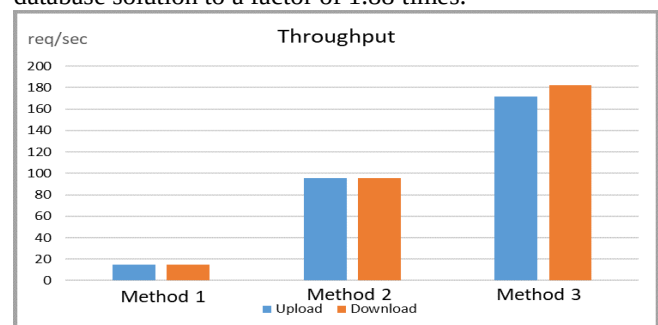


Figure 10. Performance Analysis- Average Throughput

Figure 11 shows the average response times of the three methods when the throughput is set to 100 req/s. The response times of cloud@blockchain without and with a cache are 720.69ms and 486.32ms, respectively. However, the traditional database outperforms cloud@blockchain. Blockchains require much energy to perform authentication and validation, and they are slow. All applications effectively protect privacy using low-latency operations.

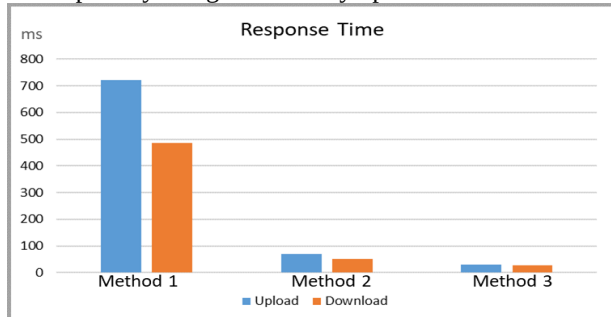


Figure 11. Performance Analysis- Average Response Time

The above feasibility assessment mainly considers the feelings of the user and the service load per unit time. It reveals that cloud@blockchain cannot compete with existing solutions. The analysis of performance provide evidence that the architecture is viable. Table 1 presents the results of the qualitative analysis. The system operations and applications features of cloud@blockchain are better than those of the traditional database solution.

TABLE 1: QUALITATIVE ANALYSIS OF TWO METHODS (CLOUD@BLOCKCHAIN WITH CACHE AND TRADITIONAL DATABASE)

| Lose                                 | Gain                             |
|--------------------------------------|----------------------------------|
| Reduce throughput by 0.45 times      | More secure                      |
| Increase Response time by 0.88 times | Easy to cross platform           |
|                                      | High anonymity                   |
|                                      | Return the right to file's owner |

## V. CONCLUSIONS

This work develops a cloud@blockchain platform and makes two main contributions. The first is an anonymous file sharing mechanism that both provides privacy and data sharing. The second is a mechanism for inspecting files to identify illegal uploads. Blockchain and cloud storage services are combined, and file sharing is performed to achieve real power dispersion and data sharing. An analysis reveals that the proposed cloud@blockchain is feasible. Although it performs 0.88 times as well as the traditional database solution, the user experience is as expected.

## REFERENCES

- [1] F. Alsubaei, A. Abuhssein and S. Shiva, "Quantifying Security and Privacy in Internet of Things Solutions," Proceedings of the IEEE/IFIP Network Operations and Management Symposium, pp.1-6, Taiwan, April 2018.
- [2] N. Zhumabekuly Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams," IEEE Transactions on Dependable and Secure Computing, Vol.15, No.5, pp.840-852, 2016.
- [3] M. Takemiya and B. Vanieiev, "Sora Identity: Secure, Digital Identity on the Blockchain," Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference, pp.582-587, Japan, July 2018.
- [4] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda and V. Santamaria, "To Blockchain or Not to Blockchain: That is the Question," IT Professional, pp.62-74, March/April 2018.
- [5] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin Organization, 2008.
- [6] R. Henry, A. Herzberg and A. Kate, "Blockchain Access Privacy: Challenges and Directions," IEEE Security & Privacy, Vol.16, No.4, pp.33-45, July/August 2018.
- [7] N. Kshetri and J. Voas, "Blockchain-enabled E-voting," IEEE Software, pp.95-99, July/August 2018.
- [8] V. Sharma, "An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV)," IEEE Communications Letters, Vol.23, No.2, pp.246~249, February 2019.
- [9] M.P. Andersen, J. Kolb, K. Chen, G. Fierro, D.E. Culler and R.A. Popa, WAVE: A Decentralized Authorization System for IoT via Blockchain Smart Contracts, EECS Department, University of California, Berkeley, 2017.
- [10] J. Singh and J.D. Michels, "Blockchain as a Service (BaaS): Providers and Trust," Proceedings of the IEEE European Symposium on Security and Privacy Workshops, pp. 67-74, UK, April 2018.
- [11] B.C. Florea, "Blockchain and Internet of Things Data Provider for Smart Applications," Proceedings of the 7th Mediterranean Conference on Embedded Computing, pp. 1-4, Montenegro, June 2018.
- [12] J.H. Park and J.H. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," Symmetry, Vol.9, No.164, August 2017.
- [13] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services using Blockchains: A State of the Art Survey," IEEE Communications Surveys & Tutorials, Vo.21, No.1, pp.858-880, 2019.
- [14] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 468-477, Spain, May 2017.
- [15] Y. Niu, L. Wei, C. Zhang, J. Liu and Y. Fang, "An Anonymous and Accountable Authentication Scheme for Wi-Fi Hotspot Access with the Bitcoin Blockchain," Proceedings of the IEEE/CIC International Conference on Communications in China, pp.1-6, China, Oct. 2017.



Jiann-Liang Chen was born in Taiwan on December 15, 1963. He received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taipei, Taiwan in 1989. Since August 2008, he has been with the Department of Electrical Engineering of National Taiwan University of Science and Technology, where he is a professor now. His current research interests are directed at cellular mobility management and personal communication systems.



Yi-Wei Ma is an assistant professor in National Taiwan University of Science and Technology. His research interests include internet of things, cloud computing and communication systems.



Chen-Jui Huang received the M.S. degree in Electrical Engineering of National Taiwan University of Science and Technology, Taipei, Taiwan.