Verifile-Blockchain Based Data Sharing

Neha Barhate[1], Nutan Patil[2], Aishwarya Devrukhkar[3], Shamali Dawarung[4], Prof. Shraddha Subhedar[5]
Department of Information Technology
[1,2,3,4, 5] Saraswati College of Engineering, Navi Mumbai, Maharashtra

Abstract- *Verifile system describes the design of a framework and implementation of blockchain based data sharing. Because of the popularity of the Internet, the integration services have gradually changed in life, such as e-commerce activities on transactions and so on. For the sake of protecting users' privacy from the malicious data which is shared by other people and leasing the pressure of the clouds, an approach of verification based on the blockchain is put forward in our system. It never guarantees whether the third-party is trust. By using the blockchain to record the hash value and other necessary information of data sharing by other people, we can guarantee that the data user received from a third-party source (such as a cloud storage platform) is the original uploaded data indeed. This blockchain-based approach of verification can effectively help users find out if the data received is the one exactly he wants. In addition, our approach will imply that the data is not the original one and that data cannot be opened or executed. The tool used are Android SDK development, Java, Eclipse in mobile applications which will be displayed when authorized person uses the software.*

Keywords- Blockchain, Data Sharing, Security.

I. INTRODUCTION

A blockchain is a growing records, called blocks, which are linked using cryptography.Viewer can view a Blockchain as a public ledger of all transactions that have ever been executed. Each block contains a hash of the previous block, a timestamp, and transaction data. It is constantly growing as completed and the blocks are added to previous blocks forming a chain. Importantly, blocks are added to the Blockchain in a linear order. The Blockchain they receive the complete and accurate information about the addresses and their balances right from the genesis block to the most recently completed the block. By design, a blockchain is refer to modification of the data. It is used to record transactions between two parties and in a proper verifiable and permanent way"

Blockchain has several advantages. First, it currently exists as a peer-to-peer network that has no single point of failure. If there is a failure in any node, the other nodes will continue to operate, maintaining the system's availability. Second, almost the documentation is digital and can be easily applied to many different applications. Third, all transactions on the Blockchain are visible to all its participants, with the corresponding increase in auditability and trust. Fourth, changes to the Blockchain are extremely difficult and in the very rare case such a change occurred, it would be visible to the other users. These advantages of Blockchain technology will eliminate third parties, lower transaction costs, and cause transformation in many industries.With the development of current Big Data technologies, it is more and more common for people sharing data or files through cloud storage platforms. Usually, people can download specific files which are shared by other people whether they know or not by searching files' name or some other keywords. When people sharing files and data through this way, there will be several methods for a hacker to harm people's privacy. In detail, hackers could not only tamper the original content of the file which people want to share but also change the original file into an executable one which contains malicious code.

To overcome this weak point, we use the Blockchain as a verification tool in verifile system to help people know whether the file downloaded is the original one or not so that they will not confused by tampered content or execute the malicious program.

What is Blockchain?

Blockchain was first introduced in Bitcoin (crypto currency) by Satoshi Nakamoto, who developed a peer- to-peer online payment system that allows online transactions through the Internet without relying on any third-party payment gateways. Blockchain is secure by design with a high byzantine failure tolerance. A blockchain stores each transaction in a block, the block eventually becomes completed as more transactions are carried out. Once complete it is then added in a chronological order to the blockchain. Blockchain was first implemented in Bitcoin application which is a currency that could be exchanged over the Internet relying only on cryptography to secure the transactions. Blockchain is an ordered data structure that contains transaction history. Each block in the

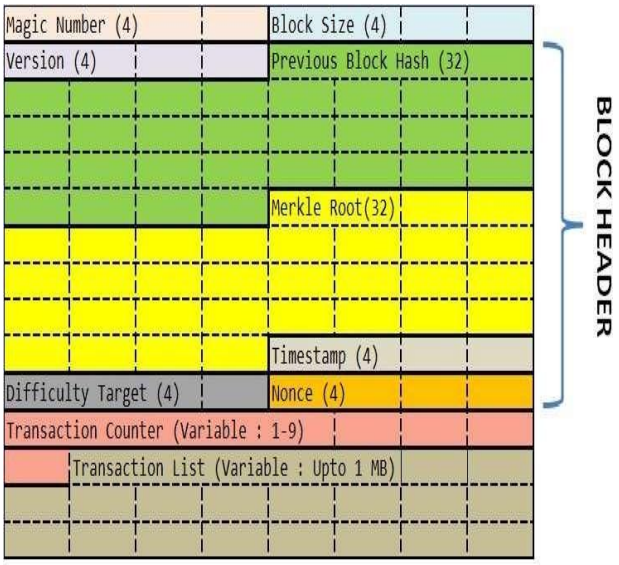

Fig. 1 Block Structure

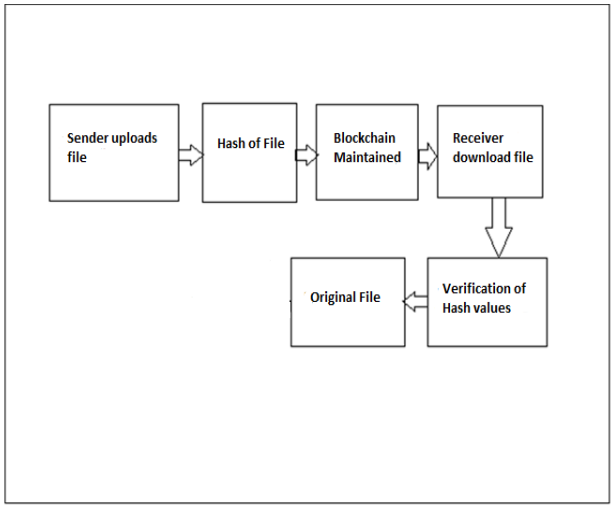

Fig2.Block Diagram

chain is linked to the previous block in the chain using its hash value. The first block in the chain is referred as thefoundation of the stack. Each new block created gets connected to the previous block to form a stack called a Blockchain.

II.BLOCKCHAIN AS A SERVICE FOR VERIFILE

Files can be downloaded by people which are shared by other people whether they know or not by searching file's name or some other keywords. When people sharing files and data through this way, there will be several methods for a hacker to harm people's privacy. In detail, hackers could not only tamper the original content of the file which people want to share but also change the original file into an executable one which contains malicious code. To overcome this weak point, we use the Blockchain as a verification tool in verifile system to help people know whether the file downloaded is the original one or not so that they will not confused by tampered content or execute the malicious program.

Design Properties:Security properties of verifile system should hold:

Verifile – Blockchain based Data Sharing" will effectively help users find out if the data received is the one exactly he wants. Therefore , the development of system is expected to be able to :

I. Identify legitimate user.
II. Secure stored file in cloud platform.
III. Avoid third party involvement.
IV. Download original file without tampering.

Verifile working:

The user will first get himself registered by providing the personal details. Then after registration the user will login into the system after proper verification. After that when user wants to upload a specific file, he selects the file and send to the particular person.In the Blockchain, each block holds the hash value points to the previous block and the hash value of the next block is calculated by the hash value of the previous block. During this procedure, other nodes in the Blockchain can check whether this hash value and the hash value created at the receiver side are same. At any time when another user wants to download this file the Blockchain system we used here will get the corresponding hash value through this latest hash value. If both values are the same, we can learn that the downloaded file is the original one without tampering. Otherwise, the file may not be the one which is uploaded by the owner and the user should leave this file alone.

Algorithm:

The algorithm of Verifile is implemented as-
Step 1 : Start.
Step 2 : User logs in Android application.
Step 3 : User selects a file and uploads a file.
Step 4 : Calculate Hash information of file using SHA-256. Hash function takes inputs and turn into outputs of a fixed size.

Once blocks are created all these values are assigned to the block. All these values are constant means once they are assigned no one change them i.e. they are immutable.

Each block in the stack is identified by a current hash value. This hash is generated using the Secure Hash Algorithm (SHA-256) to generate an almost idiosyncratic fixed-size 256-bit hash. The mostly used algorithm was designed by the

National Security Agency (NSA) that is SHA-256. It was used as the

Field	Description	Size
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypted almost unique Hash.	80 bytes
Transaction Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block.	Depends on the transaction size.

protocol to secure all federal communications. The SHA-256 will take any size plaintext as an input, and encrypt it to a 256-byte binary value. The SHA-256 is always a 256-bit binary value, and it is a strictly one- way function. The figure 4 below shows the basic logic of the SHA-256 encryption.

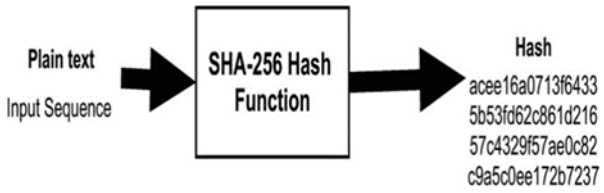

Fig3.Basic Hash Function

Step 5 :These hashes are then organized into Merkle Tree. Merkle root of hash tree placed into block's header along with hash of previous block.

Step 6:Block header is then hashed with SHA-256 producing output of complete block.

Step 7 : Use Proof-of-Work(PoW) to check whether block header's hash is valid or not.

Bitcoin protocol sets target value for block header's hash.This target value can be adjusted by bitcoin protocol.

Any block who doesn't produce a hash that is less than target value will be rejected.

For invalid hash, add one to nonce and rehash header, then check to see if that hash is valid.

Valid blocks are added to blockchain.

Step 8 : The user is able to download file and blockchain is maintained at receiver's side.

Step 9: End.

III.CONCLUSION

We conclude that through verifile system, we introduce a new verification mechanism based on the Blockchain to hold the hash value of the original file in the block. Comparing to other securely method of sharing files, Verifile may be advantageous in terms of-Firstly the operation of calculate the hash value of the file can be done offline, which decrease the risk of leaking the hash value and user's private keys. Holding the identity information by user themselves can prevent users from suffering information leak from the cloud platforms which contains user's identity information. Furthermore, by letting the verification phase apart from cloud platforms, we ease the burden of platforms so that they can focus on their core businesses. As the result, it inherits some weak point from the traditional Blockchain mechanism.

REFERENCES

[1] Yu Liu, Haopeng Chen, A Blockchain-based Verification for Sharing Data Securely, Shanghai Jiao Tong University,2017 IEEE, 978-1-5386.

[2] Huckle S, Bhattacharya R, White M, et al. Internet of things, blockchain and shared economy applications[J]. Procedia Computer Science, 2016,98: 461-466.

[3] Fanning K, Centers D P. Blockchain and Its Coming Impact onFinancial Services[J]. Journal of Corporate Accounting & Finance, 2016,27(5): 53-57.

[4] Kishigami J, Fujimura S, Watanabe H, et al. The Blockchain-Based Digital Content Distribution System[C]//Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on. IEEE, 2015:187- 190.

[5] Fujimura S, Watanabe H, Nakadaira A, et al. BRIGHT: A concept for a decentralized rights management system based on blockchain[C]//Consumer Electronics-Berlin (ICCE-Berlin), 2015 IEEE 5th International Conference on. IEEE, 2015: 345-346.

[6] Karame G, Audroulaki E. Bitcoin and Blockchain Security[J]. 2016.

[7] Matzutt R, Hohlfeld O, Henze M, et al. POSTER: I Don't Want That Content! On the Risks of Exploiting Bitcoin's Blockchain as a Content Store[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 1769-1771.