IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

# Blockchain for cloud backup system

Karthik C.
karthikcy98@gmail.com
School of Engineering and Technology, Jain University, Bengaluru, Karnataka

Chandan M. N.
chandannagaraj8@gmail.com
School of Engineering and Technology, Jain University, Bengaluru, Karnataka

Abhinandan
9abhisallu@gmail.com
School of Engineering and Technology, Jain University, Bengaluru, Karnataka

Mohammad Rayan Baig
rayanshariff7@gmail.com
School of Engineering and Technology, Jain University, Bengaluru, Karnataka

## ABSTRACT

***Blockchain Technology is an emerging technology in the software world. In order to understand the applications of the blockchain, it is necessary to understand how blockchain works. Blockchain was first introduced by Satoshi Nakamoto in 2008, which serve a Peer-to-Peer ledger for registering cryptocurrency bitcoin transactions. The blockchain is a list of records stored in the form of a chain. A blockchain is a decentralized distributed ledger which means a number of records are stored in a block and the block is added to the chain. Each block consists of a number of transactions for each transaction there will be a unique hash value, all hash values of the number of the transaction are combined and made a single hash value of the block and this follows Merkle root hash method. The invention of blockchain in cryptocurrency bitcoin solved the issue of double spending. The invention of blockchain in data backup can decrease the security complexity and duplication of the data. Rather than storing the data in one single hub that is the centralized system we can store the data in the blockchain which is a decentralized distributed ledger. In this decentralized system, the file is divided into a number of chunks stored into the blockchain which makes it difficult for data hacking and data tampering. In a centralized system if a server goes down then data is lost forever and in centralized system records can easily be altered because it does not have a backup to verify the records but in the blockchain, every peer in the network has the copy of the records and it is difficult to tamper the records. The files can be divided by a technology called Reed-Soloman erasure coding, generally used in CDs and DVDs. Reed-Soloman erasure coding allows dividing files in a redundant manner, where any 1 of 3 segments can fully recover a user's file.***

***Keywords***— *Blockchain, Decentralized, Cloud storage*

## 1. INTRODUCTION

The decentralized cloud system stores the data in the number of blocks in the blockchain that is the file uploaded into the blockchain is divided into a number of chunks and stored in the blockchain. The files are divided in a redundant manner using a technology named Reed-Soloman coding in which 10 out 0f 30 segments can fully recover the user's file. This means that is 20 out 0f 30 go offline, the user can still be able to access the file. In decentralized system data and file duplication, the eliminated completely. Before uploading the document to the blockchain each file segment is encrypted using a hash algorithm. This ensures that the hosts only stores the encrypted file segments. The decentralized system differs from traditional cloud system is that the traditional cloud storage system does not encrypt the user file before storing into their system. Cloud backup innovation technology integrates Blockchain technology in backups, allowing user permissions and verification for enterprises setting for customer services. The owner of a file in the decentralized system can give permission like reading, write and master permission to other users to access the file. A cryptocurrency can be introduced to buy, sell and rent the storage to use the store in the decentralized system.

### 1.1 Miners

Miners are members of the same blockchain who perform mining. The miners are the validators after solving a block i.e., transactions the transaction fees will be created by the blockchain itself and this process is called as Mining. Mining in the blockchain technology is the process of adding solved blocks to the large distributed decentralized public ledger of existing blocks known as the blockchain. The miners use an algorithm to solve the transactions and add it to the blockchain and it is known as the Consensus Algorithm. A block consists of a number of transactions in a single block, each transaction will be solved by different miners so that the block reward will be divided as transaction reward/fees amongst the miners. Miners will include their proofs in return for a transaction fee. Because hosts consent to all file contracts, they are free to reject any contract that they feel leaves them vulnerable to closed window attacks

### 1.2 Consensus algorithm

The consensus algorithm is the fundamental of blockchain. A Consensus algorithm in blockchain technology is a process used to achieve agreement on a data value among distributed organization or systems. In Consensus algorithm group of people or nodes comes to a common decision how blocks should be added to the blockchain. Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes. Hosts prove their storage by providing a segment of the original file and a list of hashes from the file's Merkle tree. This information is sufficient to prove that the segment came from the original file. Because proofs are submitted to the blockchain, anyone can verify their validity or invalidity. Each storage proof uses a randomly selected segment. If the host is consistently able to demonstrate possession of a random segment, then they are very likely storing the whole file. A host storing only 50% of the file will be unable to complete approximately 50% of the proofs.

### 1.3 Hashing

Hashing means giving an input data like file segment, string, number of any length and getting an output string of a fixed length. In many of the cryptocurrencies like Bitcoin, the transactions of the bitcoin ICO is taken as an input and it is run through a hashing algorithm which gives an output string of fixed length. There are many hash function like SHA-3, SHA-224, SHA-256, etc., to generate a hash value to a block SHA-256(Secure Hashing Algorithm 256) is a hash function used in Bitcoin Blockchain which converts text, number and any kind of data to a 256-bits (32 bytes) string known as the hash value. SHA-3 (Secure Hashing Algorithm) is a hash function used in Ethereum Blockchain. To calculate target hash i.e., the hash of a mined block [Target Hash= (Merkel Root Hash+Nonce)] is the formula. The target hash is the hash value of the block which is mined. More the miners in the blockchain more complex will be the target hash. Merkel Root Hash is the hash of the entire block, in a block we have more than one transaction and each transaction has its own hash value by Merkel root algorithm a single and unique hash value will be generated to a block known as Merkel root hash. Bounce is a random number calculated by brute force technique, the very first value of the nonce is zero.

### 1.4 Security

The random number generator is subject to manipulation via block withholding attacks, in which the attacker withholds blocks until they find one that will produce a favourable random number. However, the attacker has only one chance to manipulate the random number for a particular challenge. Furthermore, withholding a block to manipulate the random number will cost the attacker the block reward. If an attacker is able to mine 50% of the blocks, then 50% of the challenges can be manipulated. Nevertheless, the remaining 50% are still random, so the attacker will still fail some storage proofs. Specifically, they will fail half as many as they would without the withholding attack. To protect against such attacks, clients can specify a high challenge frequency and large penalties for missing proofs. These precautions should be sufficient to deter any financially-motivated attacker that controls less than 50% of the network's hashing power. Regardless, clients are advised to plan around potential Byzantine attacks, which may not be financially motivated.

## 2. MOTIVATION AND RESEARCH PROBLEM

The blockchain is a secured decentralized distributed ledger. For many years people were exchanging values from many technological institutions like legal systems, corporations, and marketplaces. As the society grows more complex and trade route grow more distance more formal institutions were built up like barter system, banks for currency, etc. In the early days, people were exchanging the values by the barter system and banks came into existence. As the uncertainty and complexity grow up personal control was much lower, eventually by using internet bank institutions were put online. Nowadays banks have been charging high transactions fees and it's been very expensive exchanging the values. But there is a new technological institution that will fundamentally change how to exchange value and it's called the Blockchain. As humans find ways to lower the uncertainty about one and another so that exchanging values becomes easier. For the first time uncertainty can be lowered by not just with political and economic institutions but can be done with technology alone and that is by Blockchain Technology. The Blockchain is an open source ledger the transactions are openly done with the public. If any changes to be made to the transactions then it must be done with the permission of the members in the blockchain. The Double-spending problem in a digital scheme can be solved by Blockchain technology. Smart Contracts is another advantage of the Blockchain. With Smart Contracts, the agreement between two or more organization can be automatically validated, signed and enforced through a Blockchain construct. This smart contracts eliminates the need for middle men's and saves the company time and money. So using these technologies instead of storing the files in one place it can be stored in the decentralized network.

## 3. COMPARATIVE STUDY

### 3.1 Below table is the comparison of different types of blockchain

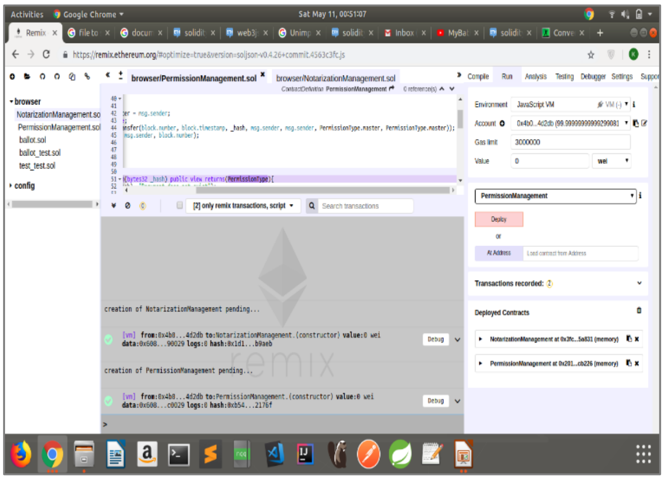
| Characteristics | Public Blockchain | Private Blockchain | Consortium/ Federated Blockchain |
|---|---|---|---|
| What is it? | Anyone anywhere in the world can read and write on the network. Data validated by every participant (node) in the network, thus making it the very secure | Permissions to read and write data onto the Blockchain a rusted' organization predetermined the owner of their controlled by a single Highly blockchain | Permissions to verify read and write on the organization predetermined nodes. blockchain controlled by a few The choice of predetermined nodes can be different for every entity on the blockchain |
| Network Type | Decentralized | Partially Decentralized | Partially Decentralized, a hybrid between private and public blockchain |
| Access | Anyone can access | Single Organization | Multiple selected organization |
| Participants | Permissionless | Permissioned | Permissioned |
| Security | Consensus mechanism, eg: Proof of Work, Proof of Stake, etc | Pre-approved participants like voting/multiparty consensus | Pre-approved participants like voting/multiparty consensus |
| Transaction Speed | Slow | Lighter and Faster | Lighter and Faster |

### 3.2 Below table is the comparison of different types of storage system

| Characteristics | Centralized Storage System | Decentralized Storage System |
|---|---|---|
| Transaction Type | Fiat-to-crypto | Crypto-to-crypto |
| Custody | The third party controlled | User Controlled |

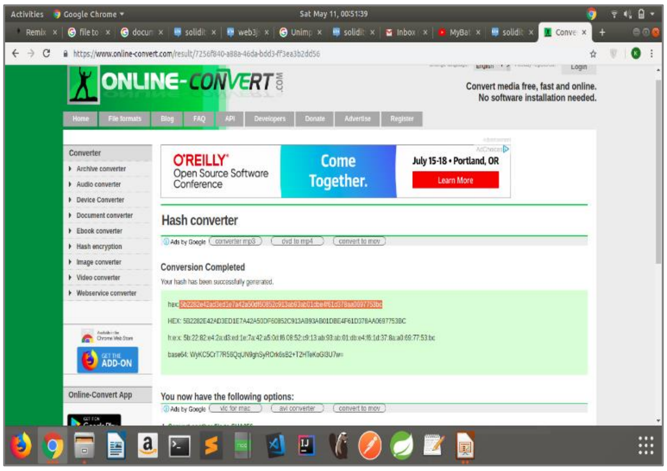
| | | |
|---|---|---|
| **Access** | Anyone can access | Only owner and permission users can access |
| **Participants** | Permissionless | Permissioned |
| **User Data Security** | User data can be accessed and can be tampered | User data is encrypted before uploading into the network. |
| **Adoption Phase** | Investment phase | Utility phase |

## 4. RESULTS



```
creation of NotarizationManagement pending...

[vm] from:0x4b0...4d2db to:NotarizationManagement.(constructor) value:0 wei
data:0x608...90029 logs:0 hash:0x1d1...b9aeb

creation of PermissionManagement pending...

[vm] from:0x4b0...4d2db to:PermissionManagement.(constructor) value:0 wei
data:0x608...c0029 logs:0 hash:0xb54...2176f
```

**Fig. 1: Deploying smart contract**



Hash converter

Conversion Completed

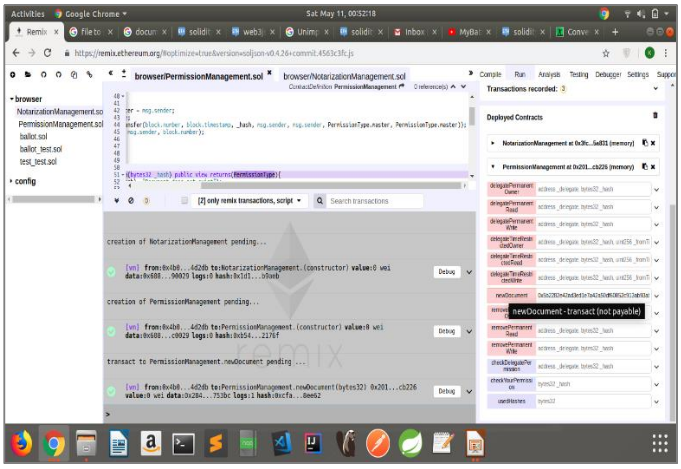
Your hash has been successfully generated.

```
hex: 5b2282e42ad3ed1e7a42a50df60852c913ab93ab01dbe4f61d378aa0697753bc
HEX: 5B2282E42AD3ED1E7A42A50DF60852C913AB93AB01DBE4F61D378AA0697753BC
h:e:x: 5b:22:82:e4:2a:d3:ed:1e:7a:42:a5:0d:f6:08:52:c9:13:ab:93:ab:01:db:e4:f6:1d:37:8a:a0:69:77:53:bc
base64: WyKC5CrT7R56QqUN9ghSyROrk6sB2+T2HTeKoGl3U7w=
```

You now have the following options:

**Fig. 2: Converting a document to Hash Value**

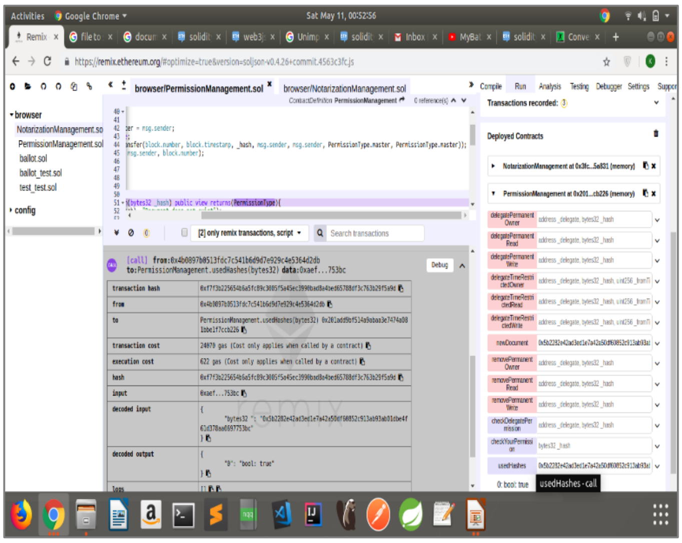
The document uploaded to the network will be converted to Hash value.



```
creation of NotarizationManagement pending...

[vm] from:0x4b0...4d2db to:NotarizationManagement.(constructor) value:0 wei
data:0x608...90029 logs:0 hash:0x1d1...b9aeb

creation of PermissionManagement pending...

[vm] from:0x4b0...4d2db to:PermissionManagement.(constructor) value:0 wei
data:0x608...c0029 logs:0 hash:0xb54...2176f

transact to PermissionManagement.newDocument pending ...

[vm] from:0x4b0...4d2db to:PermissionManagement.newDocument(bytes32) 0x201...cb226
value:0 wei data:0x284...753bc logs:1 hash:0xcfa...8ee62
```

**Fig. 3: Adding the Hash value to blockchain**

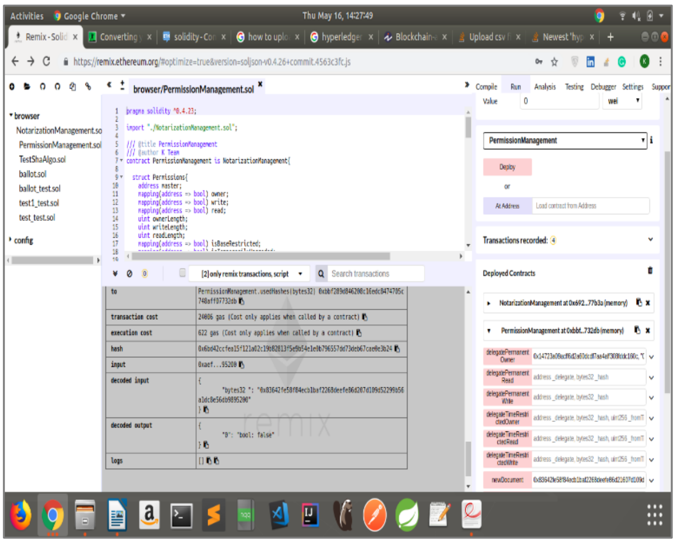
Adding the generated Hash key of the document to the Ethereum Blockchain.



```
[call] from:0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db
to:PermissionManagement.usedHashes(bytes32) data:0xaef...753bc

transaction hash   0xf7f3b225654b6a5fc89c3005f5a45ec3990bad8a4bed65788df3c763b29f5a9d
from               0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db
to                 PermissionManagement.usedHashes(bytes32) 0x201add9bf514a9abaa3e7474a08
                   1bbe1f7ccb226
transaction cost   24070 gas (Cost only applies when called by a contract)
execution cost     622 gas (Cost only applies when called by a contract)
hash               0xf7f3b225654b6a5fc89c3005f5a45ec3990bad8a4bed65788df3c763b29f5a9d
input              0xaef...753bc
decoded input      {
                           "bytes32 ": "0x5b2282e42ad3ed1e7a42a50df60852c913ab93ab01dbe4f
                   61d378aa0697753bc"
                   }
decoded output     {
                           "0": "bool: true"
                   }
logs               []
```

**Fig. 4: Checking document existence**

Checking whether the document uploaded to the network exists or not. On successful returns true.



```
pragma solidity ^0.4.23;

import "./NotarizationManagement.sol";

/// @title PermissionManagement
/// @author K Team
contract PermissionManagement is NotarizationManagement{

  struct Permissions{
    address master;
    mapping(address => bool) owner;
    mapping(address => bool) write;
    mapping(address => bool) read;
    uint ownerLength;
    uint writeLength;
    uint readLength;
    mapping(address => bool) isBaseRestricted;
```

```
to                 PermissionManagement.usedHashes(bytes32) 0xbbf289d846200c16edc8474705c
                   748aff07732db
transaction cost   24006 gas (Cost only applies when called by a contract)
execution cost     622 gas (Cost only applies when called by a contract)
hash               0x6bd42ccfea15f121a02c19b82813f5e9b54e1e0b796557dd73deb67cae0e3b24
input              0xaef...95200
decoded input      {
                           "bytes32 ": "0x83642fe58f84ecb1baf2268deefe86d207d109d52299b56
                   a1dc8e56db9895200"
                   }
decoded output     {
                           "0": "bool: false"
                   }
logs               []
```

**Fig. 5: Document Permission**

Accessing the document from the different user and adding permission using a different user.

## 6. CONCLUSION

Blockchain development is in its infancy. But already the technology is old enough that the community has bifurcated both culturally and technically. This should not be viewed as a bad thing. When the first blockchain was invented it sought to solve one very specific problem. Today, players in the space are stretching to reorganize every fact of the digital terrain. As the problems take on more definition, it becomes clear that there is not a single solution. At the same time, if the efficiencies gained by one successful blockchain project are to be shared across domains, then developers and industry managers will have to think about interoperability from the very beginning. The above proposals seek to study and identify the bifurcations in the blockchain space while finding new ways to link them together.

## 7. REFERENCES

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] R.C. Merkle, Protocols for public key cryptosystems, In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[3] K. V. Rashmi, Nihar B. Shah, and P. Vijay Kumar, Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction.

[4] Gavin Andresen, O(1) Block Propagation, https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2

[5] Hovav Shacham, Brent Waters, Compact Proofs of Retrievability, Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90-107.

[6] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Peolstra, Jorge Timon, Pieter Wuille, Enabling Blockchain Innovations with Pegged Sidechains.

[7] Gregory Maxwell, Deterministic Wallets, https://bitcointalk.org/index.php?topic=19137.0

[8] Gregory Maxwell, Proof of Storage to make distributed resource consumption costly. https://bitcointalk.org/index.php?topic=310323.0

[9] Mike Hearn, Rapidly-adjusted (micro)payments to a pre-determined party, https://en.bitcoin.it/wiki/Contracts#Example 7: Rapidly-adjusted .28micro.29payments to a predetermined party

[10] Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide.