Journal of Engineering Design and Analysis
Volume 3, Issue 2 - 2020, Pg. No. 55-58
Peer Reviewed Journal

Research Article

Secure Information Transfer using Blockchain Architecture

Suryapratim Ray[1], Aditya Bhattacharya[2], Preetam Ghosh[3], Asmita Ghosh[4], Rajat Biswas[5]

[1,2,3,4]RCC Institute of Information Technology, Kolkata, West Bengal, India.

I N F O

Corresponding Author:
Suryapratim Ray, RCC Institute of Information Technology, Kolkata, West Bengal, India.
E-mail Id:
indiasuryapritamray13@gmail.com
Orcid Id:
https://orcid.org/0000-0001-8067-3026
How to cite this article:
Ray S, Bhattacharya A. Secure Information Transfer using Blockchain Architecture. *J Engr Desg Anal* 2020; 3(2): 55-58.

Date of Submission: 2020-11-09
Date of Acceptance: 2020-12-20

A B S T R A C T

Exponential development in blockchain technology has been witnessed through the analysis of bitcoins and another important application called storj[2], which involves the concept of a distributed cloud storage. A more efficient application would be to enable file sharing through the concept of Blockchain. This would help in reducing the two-step process of uploading a file to the cloud network or drive and downloading it from the same to a single-step process of just transferring it from a sender to a receiver in a Blockchain network. Even though there are several applications that provide file sharing, it cannot match the one that is based on Blockchain technology in terms of security. Our aim is to enable a secured file sharing application by using a private Blockchain network so that it can be used within smallorganizations. Here the data is sent by encrypting the file, thereby making sure that none other than the receiver can gain access to the file.

Keywords: Blockchain Technology, Storj, Distributed Cloud Storage, File Sharing, Security, Encrypting

Introduction

The virtual currency Bitcoin has got a lot of attention since it was presented in late 2008 and implemented in early 2009. However, the main attention has been on the currency and not the underlying technology called the blockchain.[1]

Blockchain is a secure technology that enables to transfer digital data/ information through a cryptographically structured information system. In other words, blockchain is a ledger that provides a way for information to be recorded and shared by a community. That is why it is usually compared to a ledger of digital transactions.

Blockchain is a new and emerging technology and it mainly deals with the Cryptocurrency transactions where the whole transactions are fully secured and anonymous. The common example of public blockchain is bitcoins. In this project, instead of using Bitcoins, we are transferring files so that even the large files can be sent from one node to another node without uploading to any third-party cloud server.

One of the newest characteristics of blockchain is that it is a non-centralized system. That is to say, there is no need for intermediaries to identify and certify transactions. On the contrary, data is distributed through independent nodes-computers or servers that register and approve the information, without the need for a relationship of trust between them.

All the members of the chainmust validate any updates collectively.[3] Said another way, the information is only validated when the majority of the parts agrees to do it. Moreover, once the information is introduced it cannot be deleted. In this sense, the big advantage of blockchain is that, in case any node of the chain changes the register, it is automatically synchronized with the rest of the parts. Additionally, if the network of any of the computer or servers carahes, the information is not in danger, it remains intact provided that, at least, one of the parts keeps on working.

Fundamentals of Block Chain Technology

Blockchain is a distributed database that is replicated among the peers of a network. The underlying technology offers a successful way to create a trusted and tamper-proof system between mutually untrusted agents without the need of a centralized third-party. A blockchain is designed to securely store its data, make it resilient against Byzantine faults, and reach a consistent global state. It is organized into blocks that contain batches of data (Figure 1). Each block in the blockchain consists of a header and a body. The body contains the actual data (transactions), and the header contains metadata, such as a timestamp and reference to the previous block via a hash, which creates a chain of blocks back to the very first block the genesis block. Each one of these hashes takes into ac-count the transaction and metadata information contained in its correspondent block. Therefore, any attempt to alter the information of previous blocks will automatically result in a different hash, thus, breaking the chain. The participants (nodes) of the network store copies of the blockchain. Other participants can connect to these nodes and exchange the information stored in the block-chain. Blockchains are usually permission less anyone can join the network at any time without the need of authentication and can read the contents of the blockchain. However, permissioned/private blockchains are currently used in order to develop proof-of-concept systems (such as the one introduced in this paper) with a limited number of agents.

Blockchains are append-only databases: existing data in a block-chain is immutable. The data is stored at addresses, i.e., crypto-graphic public identifiers[4] which can be derived from private keys. By creating transactions signed data packages[3] the participants can interact with a blockchain. Transactions contain a sender ad-dress, a recipient address, a digital signature, a certain amount of cryptocurrency (a value stored on the blockchain), a fee that is given to the miner (see below), and an optional data field. Only participants owning the corresponding private key can send transactions from a sender address. Blockchains cannot fall back on the authority of a trusted third-party. Therefore, to guarantee consensus on the distributed storage, a consensus protocol is used. It serves as a tool for agreeing on the state of the blockchain and for securely appending new information to the blockchain. The most popular consensus algorithm is Proof-of- Work (PoW).[4]

Proof of Work (PoW)

PoW is the proof that a certain amount of computational power was consumed to solve a puzzle that allows the adding of a block to the blockchain. The process of understanding such a solution is called mining; the nodes that execute the mining process are called miners.[5] Once miners find a solution (i.e., a hash string that fulfills a

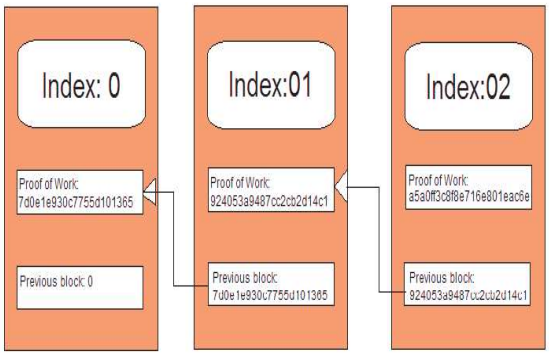

Figure 1.Blockchain validation containing data

certain target and takes into account the block's data and a suitable nonce value), they distribute the corresponding block to all the network nodes, and if the solution is valid, the blockchain gets extended with this block. While the computation of the PoW is time-consuming, verifying a correct solution is fast. Participants of a blockchain accept the longest chain (i.e., the chain which consumed the greatest total amount of calculations) as the true state of the blockchain; nodes connect to each other in a peer-to-peer[7] manner and exchange their blockchain information. Blocks can temporarily have different successive blocks, a situation that is known as a fork. This case occurs if multiple miners add solutions to the PoW puzzle almost simultaneously or if the blocks are not disseminated fast enough among the participants. These forks get resolved over time, when one chain of blocks becomes longer than the others. Transactions in the discarded chain that are not yet part of the longer chain can be included in later blocks again. The PoW guarantees that changing existing information memorized in the blockchain would require an attacker to redo all Pow computations from the block where the manipulations were made up to the current block. Therefore, as long as an attacker does not have more than 50% of the processing power of all the miners participating in the network, the data in the blockchain is immutable.[8] As an incentive for as keeping the mining process running, the solver of a puzzle receives a reward (immutable tokens acting cryptocurrency) that is comped of a block reward and the collected fees obtained from the transactions that are included in the solved block.

System Architecture

System Overview

We present an architecture for blockchain-based data transfer named as DataChain, shown in Figure 1. The node. js package extension of crypto.js has been used for the same. We utilized Merkle tree data structure[9] which uses a hash value toverify the message or data transferred betweentwo nodes. It is very important in a P2P network where we rely on unknown nodes. Consider if there are 4 messages namely 'a', 'b' , 'c' & 'd', each message is hashed

individually, then hashedvalues of a and b is combined into "ab", and thehashed values of c and d is combined into "cd".

Further these are combined into "abcd" which istop most root hash.Any changes in a single message also results inwrong hash values, and these hash values arecompared with hash values of other nodes. If thevalues are not same, it assumes that sometampering has taken place and the transactionwill not get confirmed. This maintainsconsistency as well as security in P2P networks.[10] Thus, the blockchain, a decentralized network, is used for data validation[9] and resilience.

Threat Model

To build a secure-aware architecture for collection and communication, we analyze the potential vulnerabilities in implementing DataChain. The cloud server maintains a database to cache collected data from drones but cannot guarantee that data records will remain unchanged due to known vulnerabilities in cloud operating systems. Once Data Chain is enabled, the cloud server will be able to track the data, and the auditor will be allowed to access all the collected data and data operations, as well as control commands and drone monitoring data. However, the auditor cannot be completely trusted. The adversary can potentially Acces or modify collected data, Since Data Chain's is to protect the integrity of user data, we assume that data is encrypted and stored, which is not accessible to anyone without the decryption key.

Key Establishment

Data Encryption Key KDE. After registration, the system generates an encryption key KDE,[11] for encrypting all thedata. When a data entry is created, the system encrypts thedata entry, which limits the data access only to validkey holders. Each time there is a data entry created, thehashed data entry will be recorded on the blockchain.

Data Access Public/ Private Key Pair. For data access, a public/ private key pair willbe generated, denoted as (PKDM, PRDM).[11] For somecases that the data access activity is to be recorded onthe blockchain, the private key is used to generate afingerprint from the operator to indicate the data origin, while the public key is used by others to verify the statedorigin.

Data Chain Implementation

In the system, there are three phases of data collection and transmission among the entities,including data and command transmission, blockchain receipt generation and decision making.

Data and Command Transmission

Each time there is a data record collected from the user,the data entry can be constructed as a tuple {Device ID, Time, Location, Data}. After the tuple is sent to the controller, thecontroller will forward the data to blockchain network. Atthe same time, it will send back some commands based onthe data and task. The commands will also be recorded onthe blockchain, using the tuple {Controller ID, Time, Location, Command}.

Generation of Blockchain Receipt

Once a collected data record from a user it is uploaded to the blockchain network via the controller, the event will be captured as a blockchain transaction. This provides the data management system with an ability for future validation, tracking and auditing. The record is hashed and eventually transformed into a Merkle tree node using SHA256[12].The Merkle tree root node will be anchored in a blockchain transaction following the Chain point 2.0 protocol. The use of Makle tree ofters the scalability which satisfies the vast throughput from large numbers of drones. A set of data recordswill be batched together as a transaction in the blockchain. A list of the transactions will be used to compose a new block, which will be confirmed by Blockchain nodes. When the block is validated, it will be added to the existing blockchain, makingit part of a tamper-resistant ledger.[13] The blockchain receipt contains information of the blockchain transaction and the Merkle proof used to validate the transaction. An example receipt is shown in Figure 2.

Figure 2.Blockchain validation receipt

ISSN: 2582-5607

Decision Making

With the cloud data available for validation, data auditing and decision making can be launched based on the trusted data set. The data records are stored in a time-based order and are accountable with a trusted data origin. Depending on the application scenarios of drones, either in a synchronized or asynchronized way. Data auditing is critical for detecting anomaly based on the command records from the control system and the cloud server. Based on the auditing results, effective decisions can be made to prevent and mitigate APT attacks or DDoS attacks.

Conclusion and Future Work

Since this concept is open source, we have implemented it using JavaScript, Web3.0 JS framework and Node.js framework. In future Android application for the same can be developed if the memory resource limitation can be bypassed somehow. This secure data transfer Blockchain concept can be integrated into various banking transactions to make them more secure and anonymous. Since the file is split and encoded with hex encoding, this could also create a possibility for compressing huge volumes of data into smaller sizes to further enhance the performance of file transfer in future.

References

1. Svein Ølnes and Vestlandsforsking. Beyond Bitcoin. 2016.
2. MultiChain Private Block Chain-White Paper.
3. Konstantinos Christidis and Michael Devetsikiotis 2016. Blockchains and Smart Contracts for The Internet of Things. Understanding Public Key Cryptography [Online] 2005.
4. Merkle RC. Protocols for public key cryptosystems 1980.
5. Yli-Huumo J, Ko D, Choi S et al. Where Is Current Research on Blockchain Technology? A Systematic Review 2016.
6. Wilkinson S, Boshevski T, Brandof J et al. Gordon Hall, Patrick Gerbes, Philip Hutchins, Chris Pollard 2016.
7. Euro Banking Association report. Crypto Technologies, A major IT innovation and catalyst for change 2015.
8. Back A, Corallo M, Dashjr L et al. 2014.
9. Enabling blockchain innovations with pegged sidechains. Secure and Decentralized File TransferApplication Using Blockchain ISSN.
10. Wood DG. Ethereum: A Secure Decentralised Generalised Transaction Ledger 2014.
11. Tosin P. Adewumi and Marcus Liwicki Inner For- Loop for Speeding Up Blockchain Mining Optimizing SHA256 in Bitcoin Mining ISSN:1865-0929.