JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Blockchain Distributed Cloud Storage Network Tool(BCCNT)

[1*]Ankita Sharma, [2]Rishabh Bansal, [3]Nimish Niret Soren

[1]I.T. JIMS Rohini Sector – 5 New Delhi, India
[2,3]B.C.A JIMS Rohini Sector – 5 New Delhi, India

[*]Corresponding Author: ankita.sharma@jimsindia.org

Available online at: www.ijcseonline.org

Accepted: 19/Dec/2018, Published: 31/Dec/2018

***Abstract*—** BCCNT (Blockchain Cloud Network Tool) is open source project to make cloud storage applications decentralized which will make them secure and efficient for the end users. It provides a platform for the prototype of a completely distributed network. It is proposed to develop an application which can provide a user interface for less technical/non-technical users. The cryptocurrencies functions both as a bonus and payment method. While on the other hand a separate blockchain is used to store the data for the metadata file. The application needs to be run in a P2P mesh from systems that will execute the code, present on a public chain of data instead of a central database. The main thought behind BCCNT is to offer a group of functions which makes it easy to connect Cloud & major platforms' and end users.

***Keywords*—** decentalized, cryptocurrencies, P2P

I. Introduction

Cloud storage might be a sales terms for many people and organizations which exploits the popular search for new. Cloud is still heard like a new technology as compared to web3.0, client-server integration, service. Renaming of current technology simply mis-directions. When the information is put in a cloud storage facility, then the information is transmitted via the Transmission Control Protocol from the buyer's PC to a host server. This is a consistent client-n-server model that is being used from the days of mainframe. The end-systems then replicates itself to different end-systems to follow the network standards & configuration policies, creating 3 transcripts per square meter. The present-day model of cloud storage network is operated by central facilities which measure the amount of data entrusted with non-public information which is inherently insecure is many ways. Hackers and sensors are copying or destroying the knowledge stored in the user's servers through policy, legal & technology. The difference among the above-mentioned three classes has grown clearer. The secrecy and corporate data protection are accomplished only if out of sight knowledge storage is protected from attacks emanating from each class and used in each class. If it is easily recognizable central points of attack are incorporated into the model, this can be solved by decentralization and automation. Vulnerabilities in the current cloud storage model are the payment methods that are currently widely used in almost every cloud storage provider. These payment methods are neither personal nor information secured as most of the internet-based payment technologies stores and expires the information about both, the cashier and recipient.

In today's world need of a cloud storage model that must support trust between the user and the host. Information of the end user must be secured and encrypted together with computer's file name, date, and alternate data before transferring from the end users' system to the cloud. But there is never a concentrated purpose of mistreating political vectors of attack. Payment for each information provider and the buyer can be automatic and generated in anonymous cryptocurrency. It's about time that cloud becomes a swarm made up of a huge amount of extra information filled droplets that are removed additionally as the swarm forms, shifts, and evolves. The all-embracing style principles, enables a redistributed network which is renowned from years. For e.g., Maidsafe[1] and Tornet[2] have defined doable results. But, attaining the security, quantifiability, and value potency of the redistributed storage mesh would force a code of large technical complexness. We should style the systems associate degreed network in a very secured style as we can't bet on the network or the systems themselves. Systems in between the lines of communication must join to attain the degree of superfluousness & presentation of current networks. Furthermore, our code should pass itself and while no human interference in each functional or financial view, which is associated in an unmanaged atmosphere, this is a big difference from current cloud networks.

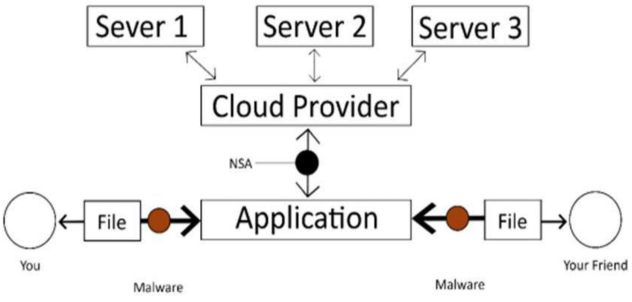

Fig 1: Standard Model for Cloud Applications

These rules are doable employing a sequence of current techs that exist like Resilio [3], Bitcoin [4], a common key encoding and cryptographic functions. BCCNT anticipates to change the evolution of a decentralized storage mesh by permitting connection with existing ASCII text file projects in an exceedingly standard fashion. This type of network should be designed additively, and with computer code that comprises of practical, simply similar components that holds a good style of tools, as well as the tools as a servicing model which current cloud service providers supplies. BCCNT will apply associate degree bonus model which is the same as the Bitcoin's incentive model. Bitcoin generators are rewarded for scientific discipline, chopping powerful information and data to the network, BCCNT will apply a new cryptocurrency like a method which procure and change cupboard place and information measure. The model inherits a free market strength of own-interest to increase networks' growth and potency whereas let remaining network be decentralized. E.g., when another quicker way of transferring a file is found, this mesh can move toward that technique till somebody discovers a fair and quicker technique. Nodes must be ready to add perpetually ever-changing and competitive surroundings.

II. OVERVIEW

BCCNT is the non-technical programmer also a development platform for the cloud network. Mistreatment the BCCNT internet UI or API, user might firmly transfer & transfer his/her files from the cloud. All docs will be encrypted, at the client side, throughout the transfer method mistreatment of non-public key provided by the host. If the host hasn't used BCCNT, the network port could supply to help the user for generation of a personal key. BCCNT connects with the network to notice accessible storage information, then transfer the docs to at least three different places in order to take care of the 3 times duplicity to consider the business customary for storage. The host or the app will increment more duplicity at an additional value. We advised a new record-registering method which will provide economical practicality for the blockchain as an information store. Once the doc is encrypted, SHA-256 hash is founded, which is a unique symbol and the simplest manner to sight file meddling. If any manipulation is found in the doc, once it's uploaded, the hash will be changed completely. BCCNT tend to use the fact in the basic platform, thus the mesh will find & look into the files, while not allowing them to get accessed directly. The consumer will be allowed to mistreat the chopping/encryption to finalize that are the received files bonafide or not. The encrypted data is going to keep in a very blockchain entry beside the three repositing locations of the doc want to generate the encrypted data.

Whole data uploaded in the blockchain is often shielded against unauthorized access and repeating by the employment of common key secret writing because all information and data getting inside the cloud is encrypted and secured, and tends to verify information through chopping, malicious entities can't spy/change the information.

A. *Protection*

Alone the host can access the decipherment key of a specific file. Furthermore, the encrypted metadata wants to establish with the file, whereas being in the cloud, is only once encrypted and the file contents stay secured. Associate assaulter cannot check the elements of the document on the cloud, although the beingness of document can be celebrated as, it is encrypted before sending, BCCNT is additionally tolerant to MITM attacks and can work on any network, even with the public non-encrypted local networks.

BCCNT will connect shopper aspect cryptography with the additional secured information, however, it is questionable Is on-browser cryptography is as secure [5]. For visible files, the normal method is enough for any other, as suggested files should be encrypted and API should pass it.

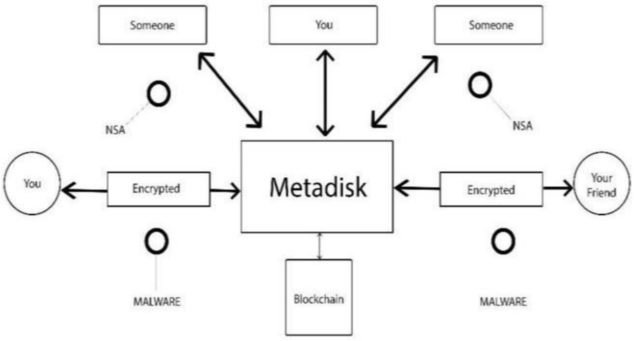

Fig 2: BCCNT Model of data storage

In this manner, whole failure of on-browser/local cryptography, & a fully concessioned BCCNT system cannot result on file's security. And this may be simply attained via local apps and tools.

B. *Redundancy*

BCCNT can run periodic checks on an information supply to create a positive file which is available. If the info supply doesn't able to grab the information, then it can be retrieved from different data supply.

C. *Improvising*

If we want to run BCCNT and some want to alter utilization of already existing free public file hosting services. There is a command line interface tool called "Plowshare" which is used to upload and download files from file sharing websites, we able to simplify the process of transfer of information to the websites. Unfinished support with respective Terms of Services of every information supply are unit liberated to BCCNT node with small pieces of information measure and maintenance for running of the node as regular information up and down between the users and the file hosting services.

Free file hosting area units probably get replace by the native disk space. That's why, BCCNT plans to integrate with another platform referred to as Maidsafe. Every platform will permit users to provide their individual storage for storing from Blockchain Distributed Cloud Storage Network Tool private individual or enterprise devices and be a member of sub urbanized chain of storage for storing.

Above mentioned platforms address issues like Cyber Attacks, Redundancy, Integrity of data. It's now seems like BCCNT is a stage skeptic. It looks for every available stage as information supply during this approach we can additionally provide finished applications to gain access to sub urbanized information platforms via simple arthropod genus of BCCNT node.

D. Toll Collection

Let's look at an example on victimization of VPS provides Digital Ocean, that can easily host BCCNT node. We assume an estimate of $5 per month, we charge the bulk of a 1TB transfer [6]. At full capacity, this works at around $0.0049 per gigabyte. Assume this in context, 100GB for the Asian country would be worth a total of $1.47 for three redundancy storage and $0.49 for full retrieval. Dropbox costs $99 per year exactly for 100GB storage. Under full capacity of 100GB for a year, this would be a price of $1.47 plus another transfer compared to $99 for Dropbox. By introducing pay as per use concept, it stopped end user from giving money to closed storage space, the user does not really need it. With time storage space grows at an exponential rate and doubles every year, it is normal for cloud service providers that files that kept for long periods of time reduces their cost per Gigabyte for its customers. So, for our full example of 100GG, cost of $1.47 per 100GB for first year in the current time. This can compete with centralized hosting services, even when the value of the storage device is halved every year, current operation prices in renting of the information center, salaries of employees, accounting prices, regularity burdens, attorney's fees, etc. Are burdened year after year, stock prices, light blur - prices for BCCNT's full information retrieval that limit their ability to fight a sub urbanized model that does not incur such costs.

E. Reducing Cost and Increasing Profit

The use of unmeasured nodes could reduce the value of information measurement more, but it's not clear, but host provider should reply to the huge size of information a BCCNT node can create. When a particular node is deleted, it does not affect communication or the data accessibility. Therefore, nodes are generally available.

This availability could prove to be a value reducer, since it is not necessary to provide overhead costs that insure against the destruction of certain nodes, but only through continued production.

An example of a use case is a dedicated server for dedicated servers like Hivelocity [7]. Your fee for a 1Gbps unencumbered subscription will allow a calculable transfer of 330,000GB for a total of $ 638 per month. After re-victimizing three redundancy and Dropbox costs, we have to generate a net profitable income like $ 9,166 every month for node engineer. The bottleneck of the network and the hidden suppliers' suppliers could cap the transmission. However, the scopes are big that we would still make a significant profit despite a 0.5 reduction in network speed.

In addition, to tell the host service provider the truth and avert misuse of common host service providers, other use case is a dedicated server vendor such as Hivelocity. Your fee for a 1Gb / s unincorporated counter allows for an estimated transfer of 330,000GB for sum money of $638 every month. Once more 3 times excess and dropbox cost for the sacrifice, we have to generate a profitable income of $36,666every month for node user.

III. Blockchain, a Backing Store

Virtual Currency [8] might be a cryptocurrency its blockchain may be a data storage for BCCNT structure. This can be for short while and can eventually get replaced with resolution on platform. With Virtual Currency, information is preserved forever in blockchain and only be retrieved using a group action hash like an associate in the Nursing Identifier. But, this guides to a tangle called the blockchain bubble. Each max node should store a duplicate of each group action in the blockchain. That means that the blockchain can quickly scale to the unmanageable size of associate in nursing, as users store only a few megabytes of knowledge. Simply saving a single show file would mean thousands of dollars in Datacoin uploading and flooding the network for the upload user. When data is saved in virtual currency system, it will almost incalculable, which is also required for knowledge that must survive, such as a reference book of mathematical principles that maintains the knowledge base but its not important or ascending information of much private type.

A. Blockchain Fuel

Saving data files themselves in the blockchain is not practical due to the bloat of the blockchain. All of us tend to fix this by storing only a tiny percentage of data for every file in the blockchain. It often set by sending a straight forward deal with the attached data. We can save the hash, the file location, and any alternate data that seems important. For confidentiality and preservation problems, we could write this data in code before loading it into blockchain.

Regardless the size of the uploaded file, this data requires 330 bytes of knowledge. We tend to add this to the typical handling of around five hundred bytes. With extra padding, we usually move one kilobyte per deal. In this case, we may save one million data till the data in the blockchain reaches 1GB in size. clarification allow us to lower the volume of data required, maltreat many chains, abuse blockchain shorten and squeezing, and largely boost the contents.

B. Advance Grading

It is so affordable for starting a file chain but not suitable for chain to manage all cloud-wide information capabilities. We need to be limited to seven transactions per second by restricting the Satoshi Mode blockchains [9]. As system operation raises, we can switch to a system where blockchain loads Merkle roots. These are cryptographic outlines of all files captured in a group action. In this approach, we could use a group action that proves the existence of millions of files. By this approach, we will straight leverage the protection of Bitcoin and/or other blockchains. At the time of writing, we need to examine Factom [10] and some different solutions.

C. Proof of Resource

It is anticipated that bandwidth will become a scarcer resource than storage after considering the Nielsen law [11], which provides for a doubling of the 2 years 1 month of high-speed urban network speeds, as well as Kryder's Law [12], which can double the storage capacity of the world for 12 months. To meet our development target of looking at coin Y as a completely new kind of cash, it needs proof of resource functions. Since many resource suppliers are connected to network, since number of bandwidths associated with Y-incremented storage may increase. In conjunction with this adaptation of the problem, the number of bandwidth-attached memories that a memory supplier should associate by a span of time to get a Y-increment of the coin rise.

It would change an open market to underline the value of CY, which supports the problem of providing CY by supplying bandwidth linked storage equipment to the network. This means that the bitcoin cost unit is partially decided by the value of the mining a bitcoin.

For the store record, all must use method of hashing a data and starting price to provide a singular hash. A node will manipulate another node to contain a random data by supplying the seed, and if alternate node contains a data, this will create a matching distinguishing hash. Full technical specifications of a proof-of-resource algorithm program are beyond the reach of this document, which describes BCCNT.

IV. RATIOCINATION

We have developed a replacement model in which a blockchain forms the support for a distributed application, BCCNT. Software/program automatically works as a P2P [13] network of nodes that execute the ASCII text file code. We offer a strong preface to a new knowledge platform. However, we tend to leave open issues related to the dispute settlement, the Cyber-attacks, and cloud platform security models.

V. FUTURE SCOPE

Why use BCCNT? We're all now familiar with the promise of Blockchain technology, and how it can disrupt the cloud business models. With BCCNT, we want to help the enterprises and individual users to simplify and accelerate the development of cloud storage networks, plus with BCCNT we are providing the cheapest and securest cloud. BCCNT is the first Indian product that will bring a distinct simplicity to the SaaS blockchain space. This promises a change in the economic equation of blockchain projects and speeding up enterprises' entire journey to adopt the technology. [14]

REFERENCES

[1] David Irvine (2017), "MaidSafe: SAFE, use case. Honest data networks",
website: https://medium.com/metaquestions/safe-use-case-honest-data-networks-3f2516610d51.

[2] Daniel Larimer (2013), "Torent: ReadMe.md, Generic P2P Tools",
website: https://github.com/bytemaster/tornet.

[3] Ilan Shamir (2017), "Resilio: P2P is Always Faster", website: https://www.resilio.com/blog/p2p-always-faster.

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," published.

[5] Tony Arcieri (2013), "What's wrong with in-browser cryptography?", website: https://tonyarcieri.com/whats-wrong-with-webcrypto.

[6] Digital Ocean, "Simple, predictable pricing", website: https://www.digitalocean.com/pricing/.

[7] Steve Eschweiler (2018), "Six Benefits of a Dedicated Server", website: https://www.hivelocity.net/blog/six-benefits-dedicated-server/.

[8] Wladimir J. van der Laan, "Datacoin - First Censorship-Free Data Storage
Cryptocurrency", website: https://github.com/datacoinproject/datacoin.

[9] Timothy B. Lee (2013), "Bitcoin needs to scale by a factor of 1000 to compete with Visa. Here's how to do it", website: https://goo.gl/FvVuaK.

[10] Crystal Wiese (2018), "Why Factom is perfect for Smart Contracts", website:https://www.factom.com/company/blog/factom-for-smart-contracts/.

[11] Jakob Nielsen (1988), "Nielsen's Law of Internet Bandwidth".

[12] CHIP WALTER (2005), "The doubling of processor speed every 18 months is a snail's pace compared with rising hard-disk capacity, and Mark Kryder plans to squeeze in even more bits".

[13] Javed I. Khan, Adam Wierzbicki (2008), "Guest editors' introduction:
Foundation of peer-to-peer computing", website: https://goo.gl/n8ws9p.

[14] Michael Dickson (2018), "Kaleido Announces the First Blockchain-as-a-Service Subscription Plans Built for the Full Spectrum of Enterprise
Ecosystems", website: https://goo.gl/nsTgv5.