Decentralized Server Using Bitcoin Cryptography and Bittorret Network

P. Thirugnanam, M.Pavithra, B.Akoramurthy

Senior Assistant Professor, UG Scholar, Assistant Professor
IFET College of Engineering Villupuram. INDIA

Abstract:

A centralized network implies a central focus of control. All the nodes in the network rely on the centralized target server.In centralized server there is a possibility of computing failure. And another issue in terms of accessing the network, sometimes it does not support the flexibility required by multiple user for varied needs. Security is one of the critical issues in centralized target. To avoid this type of issue decentralized server i.e. the nodes in the network does not have any central server to store the data. For decentralized server here bit torrent architecture can be used. Bit torrent avoids the need of the central server instead the data can be shared through the torrent. And another advantage is using Bit coin cryptography (the cryptography used in the crypto currencies like bit coin). It is based on the Secure hash algorithm (SHA).SHA is a hashing algorithm which uses the distributed hash table. The Bit coin cryptography provide more security to the decentralized network

Keywords: *zeronet, Bit torrent network, Bit coin cryptography*

I. INTRODUCTION:

Now a day's usage of internet will increase rapidly. The complex nature of the network make it to fall under the centralized network .The centralized network can have the single admin who maintains all the details about the users (including personal details) connected to the network. And the security must be taken into account because of the single admin .And another issue is the usage of internet. Centralized network must need an internet connection to share the data [17]. To overcome this,decentralized platform can be used. Decentralized platform cannot have the central point of storage so there is no need of single admin. Our data is more secure because every user can have their own data. And decentralized server does not need any internet connection [16]. Because the data can be shared through the local storage and if data cannot be in local storage the data access can also possible using six degree of separation. Decentralized network can have different type of technique to share the data like virtual ring routing etc. Here bit torrent architecture can be used in decentralized network. In Bit torrent network torrent(neighbor) will help to share the files. It is the type of peer to peer sharing. The photos, videos and the file can be shared between the peers. And for security bit coin cryptography can be used. That is the cryptography used behind the crypto currencies. The cryptography does not have any password it simply encrypt the data and store the data's in the block chain.

II CENTRALIZED NETWORK

In Centralized network the server is maintained. And all the nodes in the network rely on that single server. This type of network follows the traditional architecture called the client server architecture. Where client send the request to the server by using the standard protocols and server will retrieve the data's based on client request. So here the important thing is network connection i.e usage of mobile data and internet connection without this centralized server is impossible to access and another thing in central authority. Data base admin is responsible for all our data so privacy is one of the important issue must consider in the centralized network.

III DECENTRALIZED NETWORK

To overcome the disadvantages in the centralized network decentralized network can be introduced. Without any central admin the data can be accessed and there is no chance of data loss because every user is responsible for their own data. And there is no need of internet connectivity because the data can be accessed locally by the SQLite. SQLite is the server less database. Here the data cannot be stored and maintain by the single admin. Instead the data can be read and write dynamically on the single disk. The disk contains index, triggers and views etc.. The SQlite is said to be public domain and platform independent. Like Google chrome Zeronet is the web

browser only for the decentralized network. The Zeronet contains Bit Torrent and the Bit coin cryptography.

A) Zeronet

Zeronet is decentralized open source software creates an internet like computer network for peer to peer users. It is a decentralized web platform based on the Budapest, Hungary built in python. User will able to hide their IP address by using Tor functionality .If user visit a website in zeronetthecontent is not loaded from a single server , instead hosted from the peers who are accessing the site. And now you become a peer and startserving to other user. Sites can be served by the visitor so there is no hosting cost and no single point of failure[4]. It will also run in non-internet network like Bluetooth Wi-Fi radio communication etc.[5]. The system architecture for zeronet is explained in fig 1.1

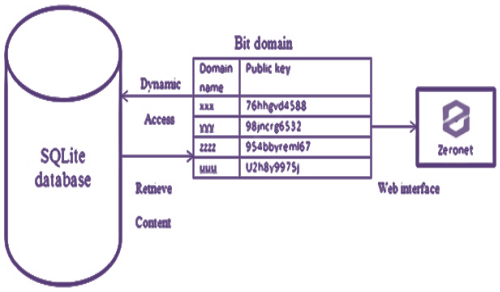

Fig 1.1 : System architecture for zeronet

B) Bit Domain

After the installation of zeronet the user must register their address into the name coin block chain. First the user must download the name coin wallet for their respective platform. Later the user have to register their domain name in name coin. The domain name must be a unique one and it is the identity for an user. Then address can be generated for the registered domain name by the block chain.

Now user have to done custom configuration to use the zeronet. For that type the following command in terminal or cmd prompt.

Fig 1.2 Zeronet key for name coin domain

After that paste the same code in custom configuration at namecoin wallet. It creates the value for our own zeronet web sites. So now we have domain name, value and address for our zeronet blog using this we have download and share the content with our torrent.

C)BIT TORRENT NETWORK

A bit torrent is the peer to peer protocol introduced by Bram Cohen in 2003for file sharing to distribute data across the network. Here seed and peers are used to sharing and downloading the file [9]. Seed is a person who contains a torrent file open to their client (let's consider you need to download the file) and the difference between you and seed is they contain the complete downloaded file and ready to sharing (seeding) the content to the peers. Peers (also called as leecher) are same as seed except the peer does not contain a complete file yet. Peer can download a file from any peer or seed. Basically still get a 100% of file the node is said to be a peer.As soon as you finished your download then you become seeders and serve to other client[10].The architecture of Bit torrent is explained in fig 1.3

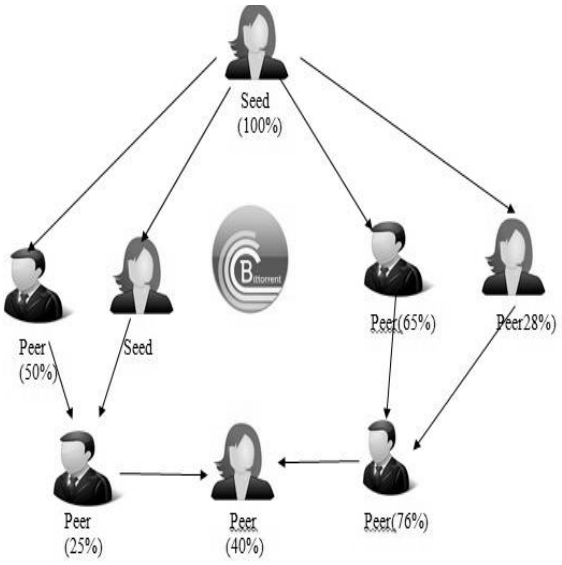

Fig1.3: Bit Torrent Network

D)BIT COIN CRYPTOGRAPHY

Bit coin is the peer to peer decentralized crypto currency that uses block chain technology [11] [12]. Zeronet uses the same cryptographic algorithm that can be used in the bitcoin. The algorithm for zeronet is SHA-256. SHA -256 can be used to generate the site address that is it uses the private key to create the site address.Like bitcoincryptography if anyone wants to create a new site in zeronetthe private key can be assigned for a user by bittorrent network [13]. And for that private key the public key can beassigned andpublic key can be visible to all the peers because it is stored in the bitdomain(namecoin block chain) based on that public key the peer will access the data. And the changes can be made only by the site owner because the site owner only contains the private key. In this way the zeronet is very safe compared [14].

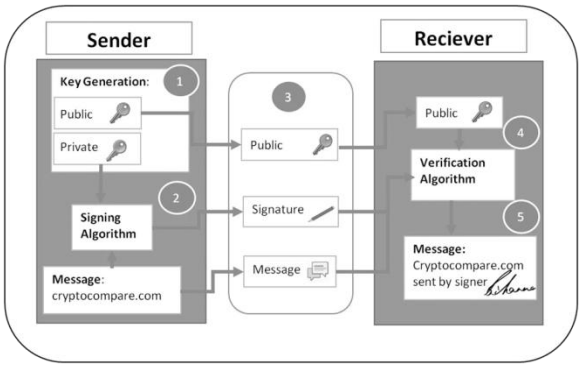

Fig 1.4 Bit coin cryptography

III IMPLEMENTATION

A)*How does zeronet works?*

After installing zeronet on your system, you can open a homepage zero hello then zeronet uses bit torrent network to find the peers that are seeding the site and download the site content from the peers and every visited sites can be served by you to different peers[15]. Sites contain a list of all files used in the site in the sha-512 hash and the signature generated using the owner's private key. if site owner modifies the site then they will signs a new list and publish it to the peers and now peers will verify the modified site using the signature they download the content and publish the content to other peers[8].When user visits zeronet the following things will happens?

1) **Gathering visitors IP address:**

First register you as a visitor. Then ask a bit torrent tracker to send the other visitors IP address [6]. This can be explained in fig1.5

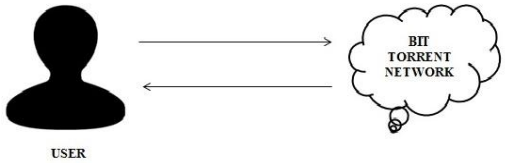

Fig1.5: Gather an IP address

2) **Downloading site's files**

Downloads a content.json file that contains the entire file name, hashes and the site owner's cryptographic signature. Verify the content.json file using the site address and the site owner's signature from the file. Downloads other files (html, css...) and verifies them using the SHA 512 in content.json file[6]. This can be represented in fig 1.6

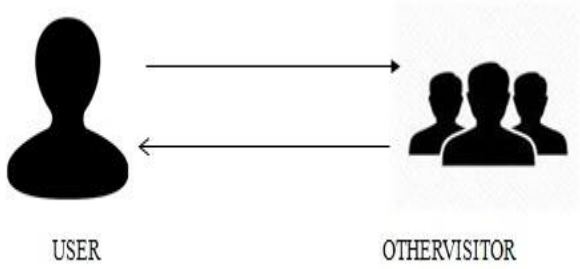

Fig1.6: Downloading the content

IV FINAL OUTCOME

If an user will install the zeronet, the initial page of the zeronet is the zero blog it contains the list of

different zeronet sites includes zero talk, zero me, zero mail, zero play, zero id , zero tube etc.. And the file list contains the list of all the torrents registered on the bit domain. From the bit register the user will download the files. First the user have to select the files what they want to download. Different bit domain register can have the same file. And the user will download the same file from the different domain members using the bit torrent technology.

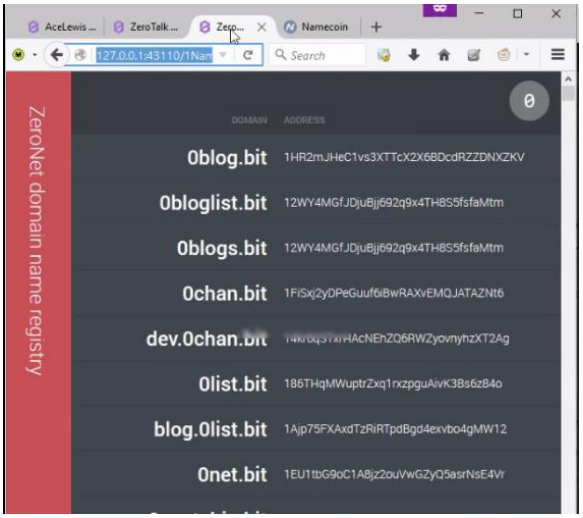

Fig 1.7 Bit domain

VCONCLUSION:

Centralized network having the single database admin may cause the security risk to the user data's. And the usage of mobile internet makes the access expensive. So to overcome this here decentralized server can be access through the zeronet(act as a browser for zeronet) and which will inbuilt the feature of the bit torrent and the bit coin cryptography. It provides more security and makes the data access more faster from its torrent. Here the data cannot stored in any central server. Instead it can be read and write from the SQLite serverless back end. Zeronet is the unshutdown able site so there is no possibility to loss our data. And the single data can be accessed from the different torrent make the site more censorship.

REFERENCES

[1] https://en.wikipedia.org/wiki/Centralized/

[2] http://aspg.com/access-management-centralized/

[3] https://en.wikipedia.org/wiki/ZeroNet

[4] https://zeronet.io/

[5] https://www.liquidvpn.com/zeronet-decentralized-web-already/

[6]https://zeronet.readthedocs.io/en/latest/using_zeronet/sample_sites/

[7] https://github.com/HelloZeroNet/ZeroNet

[8] http://zeronet.readthedocs.io/en/latest/

[9] Bit Torrent Architecture and Protocol Ryan Toole CIS 475: Vinod Vokkarane University of Massachusetts Dartmouth

[10] Bit Torrent Technology How and why it works Nicholas Lake

[11] Bit coin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto

[12] An Introduction to Bitcoin and Blockchain Technology Kaye

[13] https://medium.com/@zeronet/zeronet-bitcoin-crypto-based-p2p-web-393b5bc967e5#.gwbhno7yq

[14] https://forum.vivaldi.net/topic/6763/zeronet-decentralized-websites-using-bitcoin-crypto-and-bittorrent-network

[15] https://docs.google.com/presentation/d/1_2qK1IuOKJ51pgBvllZ9Yu7Au2l551t3XBgyTSvilew/pub?start=false&loop=false&delayms=3000&slide=id.g9a7f64c33_1_0

[16] Handbook of social network technologies and applications ,Springer

[17] Decentralized Software Architecture, RohitKhare