

ZERONET: AN OVERVIEW

M.Pavithra¹, S.Vasanth², R.Rajmohan³, D.Jayakumar⁴

^{1,2}Department of CSE, PEC, Pondicherry, India

^{3,4}Department of CSE, IFET, Villupuram, India

ABSTRACT— Internet is the basic need in today's life. Sharing of data's resources files among different group of user is possible because of the emerging growth of internet. Once the internet is only for the group of people works within an organization i.e. it is a standalone network may or may not be connected to the network. Later everything moved towards a centralized network. Every user in the network will rely on the central authority the authority must be responsible to manage maintain and update the user request. And most importantly the centralized network is established on the client server exemplarily, if particular site can be requested by an end user the request can be sent to the server through an user interface (it may be a web browser includes Google chrome, Internet explorer, Mozilla Firefox etc..) then the server gives the data to an end user. If single point failure occur in the network the centralized network will fail of course the backup of data's can be maintained by an organization which can have more complexity (time & space) and it is more expensive too. To overcome the drawbacks in centralized network this paper explains about the decentralized internet. It makes everything scattered, uncensored and anonymous. No central platform needed to maintain its data it will maintain its own data to achieve this zeronet can be introduced. Zero net is python based open source free software which makes the current network into completely decentralized network. No central authority is established to maintain its data instead of this each peer will maintain and update their own data. Zero net is simply a python based decentralized web browser.

Index Terms— zeronet, uncensored, anonymous, decentralized web browser.

INTRODUCTION

Conventional method of accessing networks is depend on the centralized server it is based on the request and response protocol if an user request the data the data can be fetched from the centralized network , web browser is act as an interface between the client and server. Here inorder to avoid an impact of centralized network in an internet decentralized network can be proposed. It makes everything independent no one will depend on anyone the idea behind this is the data present is

anywhere virtually but actually the data is nowhere. Python based software called zeronet can be used to achieve the virtuality. The network does not rely on centralized resources instead of that each user will maintain their own data the authority of the data must depend on the individual user who rely on the network. It makes an user interface decentralized instead of network. The zeronet is said to be an decentralized web browser and it is an open source python based software here the user can create their own site without much effort and they will be able to maintain it. They will act as an owner for their own data every other user will be able to access the data but no one will change the data. The site creation is very easy simply download and extract the open source package available over an internet. Decentralized is an emerging technology it simply reduces the cost of centralization and reduces the fear of third party to maintain and updates the user data. And decentralization must create a major impact in future technology growth because now itself many countries will start to chain their environment towards decentralized network.

1. ZERONET

Open source decentralized browser which communicates by using different peers without depends on any centralized server. Here peers are said to be different user connected through an internet it changes the conventional way of accessing an internet into a peer network. Zeronet works similar to torrent network i.e. no internet. And the content accessed by an user does not fetched from any central server instead of that it can be loaded from the different types of peers that can be served across the network. So it is clear that the site cannot be hosted from single server there is no hosting cost needed and if one site fail the network can still be served by the different types of seeds present in the network. Zero net does not have any specific topology and it is based on the bit torrent network. It also protects the site to be censored by a government and DMCA organizations. And zeronet is uncensored network defines the site in the zeronet can be identified through an unknown name (uncensorship). And in zeronet the sites cannot be identified through an IP address, it can be identified through the public key and public key is a unique identifier for the different sites. Zeronet serves

different sites includes zeroplay, zeromail, zerotube, zerotalk, zeroblog etc.

A. Core concept behind zeronet

Bit domain is the concept behind zeronet. Once an user download the zeronet based on their system platform they unzip the downloaded bundle and install the zeronet. Bit domain will register an user identity in zeronet . The bit domain registration can be done as follows

B. Steps to register bit domain

1. Download namecoin wallet (name coin is one of the crypto currency based on the block chain)
2. Enter new name for your domain in manage name tab and register your domain name for zeronet.
3. Configure the zeronet address to configure select tab custom configuration and enter the content.json file in custom configuration.
4. Content.json file present in the downloaded zeronet package from that we have to select the subdomain of the site what we want to create (for example if an user want to clone zerotalk and zeroblog alone they want to create the content.json file with respect to zerotalk and zeroblog) content.json file can be illustrated in the figure 1.1.
5. If content.json file is registered in a bit domain then an user name is registered in the zeronet site.

```
{
  "name": {
    "formatted": "ZeroNet project"
  },
  "bitcoin": {
    "address": "1QDhxQ6PrUza21ET5fYUCPqdrw8onnFqX"
  },
  "zeronet": {
    "": "1EU1tbG9oC1A8jz2ouVwGZyQ5asrNsE4Vr",
    "blog": "1BLogC9LN4oPDcruNz3qo1ysa133E9AGg8",
    "talk": "1TaLk3zH7ZrskJvrh3ZNCdVGVk3usPKQ"
  },
  "na": {
    "na1.domaincoin.net"
    "na2.domaincoin.net"
  }
}
```

Fig 1 Content JSON For ZeroBlog and ZeroTalk

2. How Zeronet Works

Once a user registers their domain using namecoin wallet they get an identity to access their own zeronet sites. They get their blog and talk websites in their

hosted system. If they want to get their own sites for example if they want to create their own blog based on their interest it is also possible by using the zeronet. Site creation can be done through the following steps.

A. Steps to create zeronet sites

1. Clone the zeronet site i.e. if u want to create zeroblog clone the zeroblog and update it.
2. Once the update was done, open zero bundle in command prompt.
3. Type **zeronet siteCreate** in command prompt this will create private key and public key for registered bit domain. This can be exemplified in the figure 1.2
4. **Have you secured your private key** enter yes for the above query if command prompt display an above question the site can be created.
5. Copy the owners site address generated in the zeronet bundle.
6. Again if you want to know the public and private key of your domain enter your identity address in wrap wallet it will automatically generate the public and private key based on the scrypt and SHA algorithm.
7. If peer wants to rename the public address means they change it because the public key (public address) can be used to access the particular site through this the data can be viewed and identified.
8. Once the user creates site they will publish the site by edit index.html file present in the zeronet bundle.
9. Only the owner of the site will edit the site because owner only knows the private key of the particular site.
10. Through that private key only the site can be edit. So unknown peer cannot change the user's data.

```
C:\Users\Alex Lewis\Downloads\ZeroBundle>zeronet siteCreate
Starting Zeronet...
- OpenSSL loaded, version: 01000201F
- Patching sockets to tor socks proxy: 127.0.0.1:9050
- Generating new privatekey...
-----
Site private key: 534t
!!! ^ Save it now, required to modify the site ^ !!!
Site address: 1Fs9V1jKmChrDcklksorHEQ9HzqBqCknpoll
-----
Have you secured your private key? (yes, no) >
```

Fig 2 Zeronet Site Creation Using Command Prompt

By using the above steps every peer will create and publish their own sites in the zeronet network.

3. ZERONET TORRENT

Zeronet enabled TOR (The Onion Router) network i.e. it hides an original internet protocol address of the user by two level of encryption. If an user sends a data over the internet traffic it done the encryption by using elliptic curve cryptography (which immune to brute force attack) once the first level of encryption is done the encrypted data will again enter into a rely node here second level of encryption can be done using the same cryptographic algorithm and then the data will move towards the recipient now, destination knows only its previous node the origin of data can be difficult to identified. This is how tor network hide user IP address from the network. Zero net also offers this kind of anonymous network which hides user identity from different peers in the network. The TOR can be enabled by simply entering the tab present on the right side of the zeronet sites. TOR architecture contains three types of layers includes Guard , Middle, Exit. Initially the data send from the sender will enter into the guard here first level encryption will occur and guard is also said to be an entry node which can be randomly chosen among the different numbers of peers exits in the network. Once the middle node get an encrypted data which could also be chosen randomly, the middle node again done the second level of encryption and send it to the exit node. And finally exit node will unencrypt the data and send it to the destination node. This level of nested encryption is said to be an onion router network. The TOR network can be illustrated in the below fig 1.3

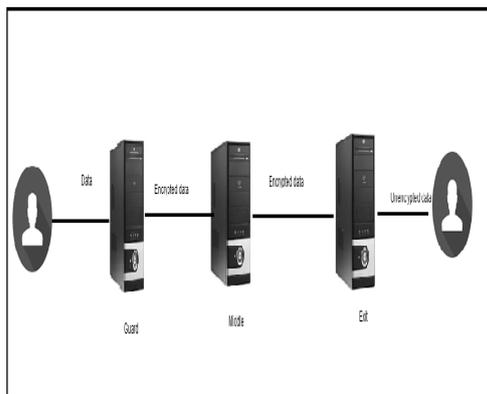


Fig 3 TOR network

And bit torrent network can be used to download the data from the different peers. The network contains two types of nodes namely seeds and peers. The seed contains 100% of data and once the node can have the full downloaded data this will act as a seeding node to other peers. The network structure for bit torrent is illustrated in the fig 1.4.

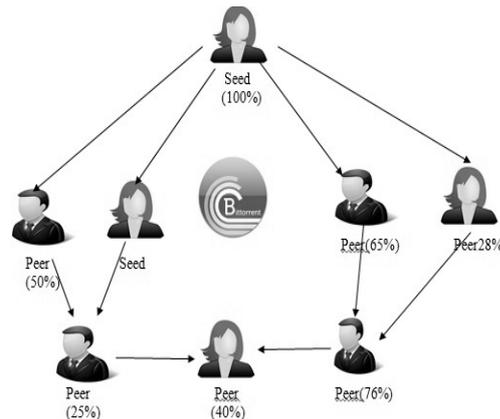


Fig 4 Bit torrent network

4. ZERONET Sites

- A. **ZEROBLOG:** Once you publish your blog in the zeronet site multiple peer will access the data from the blog through the public address site. And the site can be updated automatically.
- B. **ZEROMAIL:** It is a decentralized messaging site. In order to improve privacy end to end encryption can be used in zero mail. Initially user has to create their identity in zero mail as like the normal Gmail. Using AES 256 the message can be encrypted.
- C. **ZEROCHAT:** It is a real time chat application which can create their own messages and distribute messages over the network. It is a server-less chat application and records can be retrieved in real time
- D. **ZEROME:** It is twitter resembling societal network where the user can store data's and post their command over the network.If user wants to craft their personal sites it is also possible by using zeronet.

5. CONCLUSION

Zeronet makes everything as a decentralized network. It changes the future internet into a decentralized network and the security for the network is provided using bit coin cryptography. The block chain is used as a security

for zero net networks. Block chain is a highly secure decentralized based database which is transparent to every user in the network. But the data cannot be edit by the user the data can be changed only by an owner. So zeronet is highly secure and uncensorship network which can be easily accessed by an end user.

REFERENCES

- [1] Decentralized Server Using Bitcoin Cryptography and Bittorrent Network. IJETT , M.Pavithra, P.Thirugnanam, B.Akoramurthy
- [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>
- [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
- [18] K.Jayasri, R.Rajmohan, D.Dinagaran, “.Analyzing the query performances of description logic based service matching using Hadoop”, IEEE conference, DOI:10.1109/ICSTM.2015.7225382, pp. 1-7, May 2015.
- [19] R Rajmohan, N Padmapriya, SKV Jayakumar, “A survey on problems in distributed UDDI”, International Journal of Computer Applications, Volume 36– No.3, December 2011

