The Dark Web

-to communicate anonymously

-By Team Nikist

Ch-1

INTRODUCTION TO THE DEEP WEB

In this series of chapters,
you will get to know all
about the deep web.
Basically, deep web is a
major part of the internet.
And it consists of
information that you cannot
normally get access to by
searching it on any standard
search engine.

Many times people are confused between Deep web and dark web but these are not the same things, these two are a completely different concept. Here we are also going to discuss about the differences between the surface Deep and dark web.

Further in this series, you will get to know how to create a secure environment, all the precautions that will be needed to take while browsing on the deep web and also you will get to know how to configure multiple Linux distros on the Windows. At the end, you will be able to configure some of the famous security based operating systems like Qubes OS and Tails OS.

Now let's start with what exactly is Deep web. It makes reference to anything on the Internet that cannot be found using a search engine. You may also have heard deep web by other names as invisible web or hidden web. Basically, it is a part of the World Wide Web but due to some reasons, the standard search engines have not indexed the contents of the Deep web.

Web crawlers also are unable to index its contents. It is approximated that 90% of the whole internet comes under Deep web only 10% is the surface web what are indexed internet that you use usually.

Now let's go further and see the difference between Clear, Deep and Dark web. Clear about the surface web all that information and each and every site that you use every day for example Google YouTube Bing etc. You can easily share access of that particular page through a link.

The Deep web consists of anything that needs an authentication or has security to access. These are Private information like emails dropbox and social media and all those information that are unable to be accessed using web crawlers.

In simple words you cannot find the information in the Deep web by searching it directly on any standard search engine, just like you cannot go to Google and search for any email recipient name you will not get any relevant result.

Exploring The Hidden Internet

Deep web is a part of the surface web only but it needs a type of authentication or some credentials or something to get access to it. The Deep web may contain financial records, government resources, scientific reports, medical records, legal document, subscription information and other such type of personal information.

DEEP WEB

And the dark web contains information that is purposely hidden. Security reasons are not obligatory but it requires Special software to access the information in the dark web. Browsers like Tor especially designed to access the contents of the dark web. In the dark web, there will be illegal information drug trafficking sites, private Communications, political process and usually Tor encrypted sites.

So this is all for the first chapter hope you have a clear knowledge of what is the deep web. Head on to our next chapter to read about the common myths and misconceptions about the Deep web, you will also get to know about how tor works and what is pgp?

NIKIST

ch-2

Myths and misconceptions

In this chapter let us burst some myths and misconceptions that people have about deep web. We will also get to know how 'Tor' works and a brief description of PGP.

Let's head on to all the misconceptions first.

Many people believe that the Deep web has an illegitimate entrance. This is not true, deep web is accessible to everyone, only some countries have censorship on the access to the Deep web.

It is not dangerous or illegal to access the deep web. In fact, it is considered to be safer when it comes to the identity and thefts.

Not every website on the dark web is dangerous only some malicious websites are which are targeted to harm anyone.

It is a very big myth that using Deep web is a crime and only criminals access the deep web. But the reality is, in everyday life, Deep web is used by more than 2 million people across the world for communication and sharing information. And 2 millions can't be criminals, right.

The Deep web has all informative sites rather than malicious sites you will only get stuck on any malicious website only if you intend to do so or intentionally search for one.

NIKIST

Now let us know about how the dark net or the Tor search engine works. In very simple words door is collection of networks that are used to connect to the Deep web or the dark net basically by the means of onion router.

Let's see how Tor exactly works. Basically Tor is a string of proxy that is used to anonymize communication. Tor uses the Tor browser to perform encryption using onion routing.

NIKIST

So the client, which basically will be you, will go through an entry node which is the permanent node. This node will connect to any random node in the Tor network through an encrypted Tor connection in the Tor network. Then that node will again connect randomly to any other node and finally will connect to the exit node.

You are encrypted by Tor until here and while the data goes from the last node to the destination server in which the website you want to visit is hosted, you will not be encrypted by the Tor. This is how exactly the Tor works.

Now let us get into the third part of this chapter.

You will get to know about the PGP which is an acronym for pretty good privacy.

Basically PGP is an encryption system used on the Deep web. If you want to communicate safely and securely across the Deep web you should have a good knowledge of the PGP system.

PGP or the pretty good privacy is a technique to encrypt messages online. It is used to encrypt texts, emails, files and many more information on the Deep web.

NIKIST

Generally it is used in the Deep web to share information that is sensitive or private. You have already heard about the military grade encryption the PGP is almost similar and is very close to the military grade encryption.

Now let's see how the PGP works.

Basically what happens here is there are two person A and person B. Both of them have a public key and private key. The private key of person A is visible to only A and its public key is visible to everyone and vice versa. Now, when the person A sends a message to the person B. It encrypts that message with person B's public key and its own private key.

And when the message is received by person B, it will be decrypted by person A's public key and person B's private key. This is how the encryption and decryption of data takes placed and the PGP system works like that.

So this is all for this chapter. Head on to the next chapter to learn about setting up an environment for deep web.

how to setup the most secure environment for Deep Web.

In this chapter you will get to know how to setup the most secure environment for Deep Web.

First of all, do not use windows on the Deep Web; there are numerous reasons for not using the Windows OS. Windows is the most popular OS in the World; therefore it is likely to be the most targeted OS by hackers in terms of its weaknesses. There are increased vulnerabilities and exploits targeted at the windows operating system because of its vast user base.

Inherently by design Windows is less secure in terms of anonymity and leaking of personal data and information. It is the best Operating system but it also has its pros and cons so in terms of Deep web it does not go well as windows is less secure and can be targeted very easily.

Let's get to know how to install Tor on your windows.

First you have to download and install the Tor project and then search for Tor browser and then download the Tor browser. You get option for languages and also versions for the different OS that will be Windows, Mac OS and Linux with 64-bit and then after download it will ask you to save the file.

After saving, go to the downloaded folder and install the Tor browser. It will take you to the install wizard and then extract it and then start it. There in the network setting for the Tor browser it will ask you to provide information about your computer's Internet connection.

There will be providing you with two options which you can choose according to your preferences. Then connect to the Tor browser it will take some minutes or more depending on your Internet connection.

After that your Tor browser will start, then we will check if it is connected to the Tor browser by writing in the search box "check.torproject.org" is a website which checks the connection, and it will show whether you are configured or not and also it will also your IP address accordingly.

In next part of this chapter, you will get to know about different OS for Tor browser.

As we read in the introduction part about Qubes OS to use Tor browser as it is very secure to use Tor browser. Firstly, let's install Qubes OS, the website you will get by searching Qubes OS. Then go to the website and download the OS and install.

QUBES OS

A REASONABLY SECURE OPERATING SYSTEM

What is Qubes OS?

Qubes OS is a security-oriented operating system (OS). The OS is the software that runs all the other programs on a computer.

Some examples of popular OSes are Microsoft Windows, Mac OS X, Android, and iOS.

Qubes is free and open-source software (FOSS). This means that everyone is free to use, copy, and change the software in any way. It also means that the source code is openly available so others can contribute to audit it. It is the best OS available today and its best for security purposes even according to the experts.

You can run Qubes OS either on Flash drive or other hard drive or on virtual machine in windows. But it will be good if you install it on flash drive and you can use the installation guide. It will show you to download Rufus. Install Rufus and then run Qubes OS on it. In Rufus select all the required or asked option accordingly and then press on start.

You can also go for VMware for that download VMware and install it and then set the the Qubes OS and then select your OS properly and then save and then it will ask for disk capacity and then customize your hardware. After all the settings, it will start to install the Qubes OS on VMware and then set the Qubes OS.

There is also Tails OS for Tor browser. Now, what is Tails OS?

Tails is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you ask it explicitly.

It is a complete operating system designed to be used from a USB stick or a DVD independently of the computer's original operating system. It is Free Software and based on Debian GNU/Linux. Download and install the Tails OS on your either USB Flash drive or VMware and it will also ask you to install from windows.

Tails OS is better than Qubes OS as it is easy to use though Qubes OS is more secure but it is little hard for beginners in compared to Tails OS. Tails OS will give you more anonymity and will hide your serial number of network cards using Mac address spoofing. Tails OS already comes installed with Tor browser as it uses the onion router services. After setting the Tor browser then run it.

You can also use Linux distro for Tor browser it is an OS which is Linux distribution. You just have to download any version of Linux and install it. After that, set it in VMware and then do the setup process.

Setting the Linux now, download the Tor browser on the Linux and then extract it and install. It will configure itself and you just have to connect and then check same as you have done in windows.

So this is all for this chapter. Let's go to the next chapter and learn how to use the deep web.

Ch-4

deep web and how to use it.

Best Deep Web Search Engines

In this chapter let's get to know more about the deep web and learn how to use it.

Deep web is Tor browser in which all the urls have .onion extension except those which can be searched on clear web or surface web, they have .com or .org, etc. extensions. The search engines in the Tor browser have all the web address which has .onion extension. It has many search engines options.

Let's look for Tor browser's interface and security features. Tor browser is basically has security regarding its users. If you maximize the size of the Tor browser, it will give you warning regarding it saying to let the browser window remain in its original size otherwise the browser will be able to determine your window size and can track you down through your resolution of the device.

You can select a new identity by clicking the onion icon, after that when you search in the search engine like Google, it will give different IP address, then again by clicking on the onion icon you will get to know about the IP address or Tor circuit you are currently using. You want to change, go to settings and set the security level for the sites.

It has three security levels low which is default, then medium and then high. All the three have different level of security. If it is low, then it will be like clear web, if its medium, then it will provide you with some security and if you set it to high, it will disabled some scripts as a security so that your anonymity is maintained.

The DuckDuckGo is the best search engine because it's anonymous and does not track any of your search queries. Most of the common problems you will have are that most of the links do not work. Do not go for torrent sites, as it may reveal your location.

Now, in next part of this chapter let's get to know about the best search engine of the deep web or dark web. One of the best search engines is AHMIA which has very clean design and interface, it gives result in 0.5 seconds, it gives statistics and about the sites about how old they are or not.

The second best search engine is Candle which is actually inspired from Google colour scheme. It is very easy and have very good interface. Third one is Not Evil which is simple but does not customize everything properly.

Fourth one is Grams which allows you to search the dark web or deep web markets. Last one is Torch which basically very simple but it takes time and also it does not gives you knowledge about the last modified site which can lead us to inaccessible and blocked or non-existed sites.

Best Email providers on deep web or dark web is very secured and gives us anonymity and does not track us that how many emails we send in a day. First one is ProtonMail which is actually on the clear web too but does not work properly there and it gives free service for the public good and also have facility for online privacy by selecting a paid account and it is an open software.

Second one is Torbox which is hidden as it is only available on Tor. It gives us good encryption. Next one is Bitmessage which is a service to connect bitmessage to email without any tracking and have no advertisements as it uses HTML.

NIKIST

The last one is Mail2Tor which is a free anonymous e-mail service to protect your privacy. It allows anyone to send and receive emails anonymously via webmail or with an email client but is a bit slow. It is also accessible only on Tor browser.

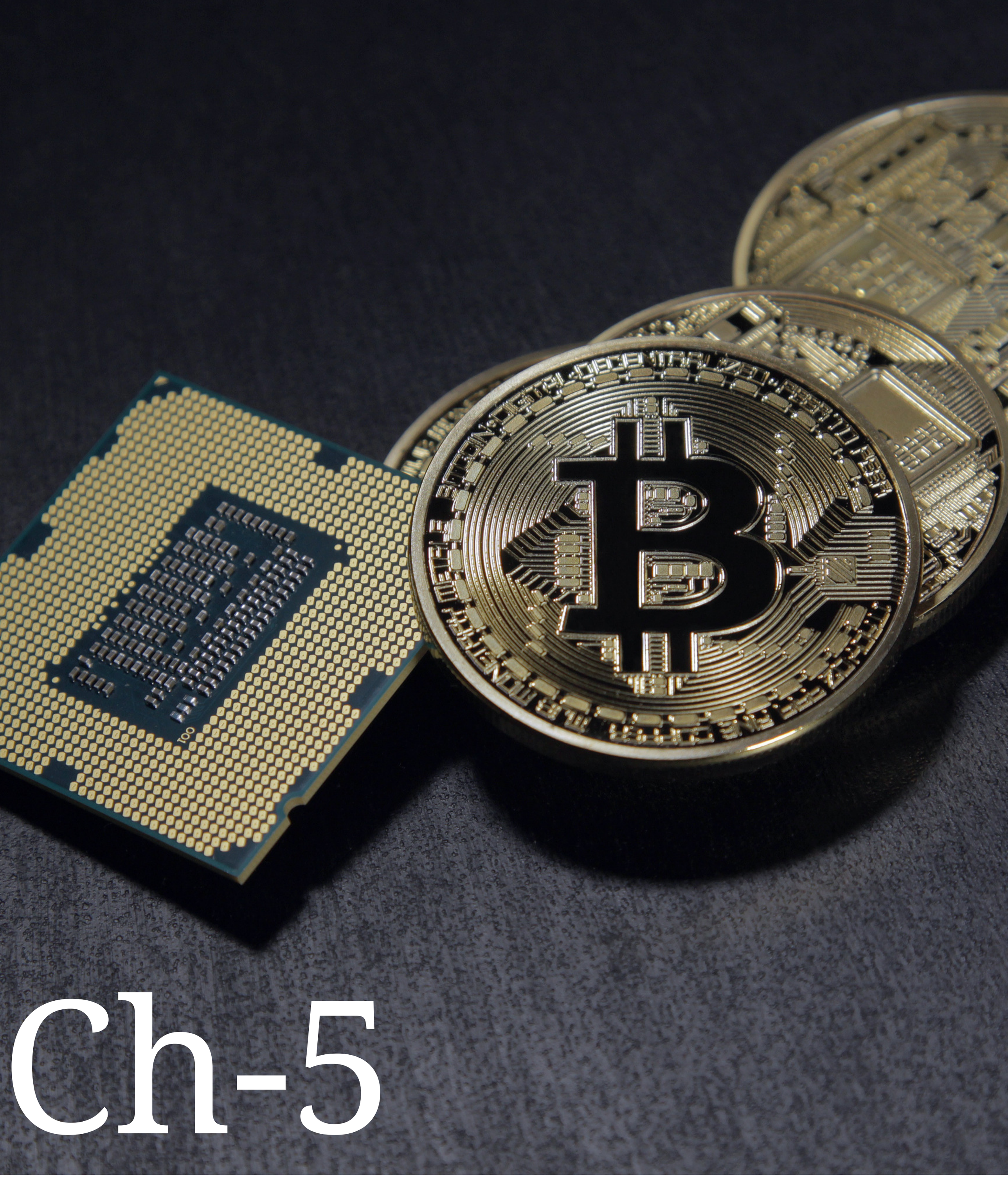
NIKIST

Now we are going to see the best social networking sites and forums on the deep web or dark web. First is Galaxy2 which is actually the best social site on the deep web and is easy and clean as it does not contain any malicious or disturbing content in it.

Then we have ChatTor which is a chat room allows to chat anonymously with anyone randomly just by using a random name.

Next one is Facebook which we all are already aware about as it is available on clear web also but here it has its .onion and says that here it does not tracks anything but we cannot think whether it is true or false as this thing is not mentioned in its terms and conditions.

The last one is Intel Exchange which is basically a forum where we can discuss about the interesting stuff deals with science technology.
So done for this chapter, now, head to the next chapter which is about the bitcoin on the deep web.



Ch-5

Bitcoins and their use on the dark web or deep web

In this chapter we will learn about the bitcoins and their use on the dark web or deep web

First let's learn what is Bitcoin? Bitcoin has abbreviation and that is BTC. Bitcoin is basically a decentralized currency which essentially means it is not physical currency; it is used on the internet. It is the most preferred for payments on the dark web and it is preferred because of it anonymity capabilities.

Bitcoin is not completely anonymous, however it is much more anonymous compared to your credit card. It is a very erratic currency and is highly volatile and unpredictable, so investing is kept to a minimum.

Let's discuss about Bitcoin terminology.

First is bitcoin wallet where you can store bitcoins for its later use. Then comes bitcoin address which is an alphanumeric key that will be used to send and receive bitcoins.

Blockchain is a list of blocks that have been mined since the start of cryptocurrency. ATM is the location where you can buy your bitcoin with real cash. Bitcoin mining is a generation of bitcoins in exchange for solving cryptographic problems using computer processing.

Bitcoin value equals to 2218.47 US Dollar. It started it value in 2013. It has erratic graph so it is not god to invest in it.

What is blockchain?

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data.

Let's get to know about bitcoin wallet and how to choose them and how to set up bitcoin wallet. First option is Coinbase which is actually the leading bticoin service in terms of exchange and it has high user base which means it is trusted but it cannot be fully trusted as it does not deal with bitcoin wallet in appropriate way as it basically knows your bitcoin address that basically means

it can identify you by your personal information through that bitcoin address that can really breach anonymity and anyone can easily get to you and transactions you have done but it is beginner friendly. It is currently supported in only 32 countries and not worldwide.

It basically operates online so you have to create an account an then you will get your bitcoin address and you can start your transactions. It can be accessed in Android and iPhone too.

Second is Bitcoin Core which is basically keeps bitcoin decentralized, tyhe reason why bitcoin was created. It also allows doing the transactions with your anonymity and it can be installed directly on the desktop. It is the stable programmed to decide which blockchain contains which transactions.

Its downfall is it does not work on the internet and cannot be installed on mobile devices but this is also a god thing. Download and install it on the desktop. After that you can decide where to store bitcoins. While transaction it will give bitcoin address with QR code.

There is also a blockchain.info which is one of the best, it is same as bitcoin core but is online. It gives us same anonymity.

There is good user interface and has god security features.

Now, let's know about earning free bitcoin through bitcoin faucet websites.

This bitcoin faucet website is t exclusive to bitcoin but it also works for others. What are faucet websites?

A faucet website gives out bitcoin or other cryptocurrency for free in exchange for a simple task for example; watching an AD video or reviewing sites. They will pay out a very small amount of bitcoin or other cryptocurrency.

They usually pay out in small amounts called Satoshis which are equivalent to a millionth of a bitcoin. A Satoshis is the smallest unit of bitcoin : 0.00000001 BTC. Their business model is focused on advertisement revenue. There is a certain time limit/waiting period when it comes to withdrawal in order to prevent bots and spammers.

The best faucet websites are available. First one is Freebitcoin, it gives bitcoin by just referring the website to others for that you just have to login. It is very well designed website.

So that's all for this chapter, let's head to the next chapter where you will learn to install and configure pgp on your windows.

The best faucet websites are available. First one is Freebitcoin, it gives bitcoin by just referring the website to others for that you just have to login. It is very well designed website.

So that's all for this chapter, let's head to the next chapter where you will learn to install and configure pgp on your windows.

Ch-6

PGP

In this chapter you will learn to install PGP on your windows.

PGP is a Pretty Good Privacy or Pretty Good Protection.

For setting up PGP, we have to install and setup GPG.

Open your browser and browse for GPG4win and download it, then run the setup and in one step check GPA and install.

Open GPA now and set Key manager and generate key and then put a pass phrase, it is very important to remember passphrase. It will show you a public key to communicate you through this only.

To communicate, when someone will write message they will encrypt it with the receiver's public key ID and then you will receive it in a PGP format then you will decrypt it using your pass phrase and then only you will be able to read it.

Basically, PGP works like person A wants to send message to person B. Then person A will write a message and then encrypt it person B's public key ID then send.

NIKIST

After that person will receive it and will decrypt it using its private key and then only can read the message. In this way the communication can be done in PGP.

So, that's done for this chapter, now let's head towards the next chapter which explains how to create and host a deep web website.

ost Deep We
Dark Websi

how to create and host a deep web website.

In this chapter, you will learn about how to create and host a deep web website.

First go to the terminal and head to the root of the OS. Then install the Tor unit and then browse through directories and list the Tor folder.

Edit the file Torrc and then type hidden service directory, then directory name.

After that mention the hidden service port and then go to adapter using other terminal and then take your IP address and paste it and then setup and then install apache and go to your directory, then your folder and take your hostname which is basically your deep web link.

After this get your HTML code and give your website name ad your other preferences, then save it.

Open your TOR browser, connect it and then copy the link to the search engine a search and you will get your website.

That's all for Now.

we hope you like this short and simple ebook. please send us your review on our instagram page