3
The Future of the Dark Web

In the following chapters, we'll discuss the technical side of accessing the Dark Web.

When I start using any technology, I try to think what it will look like in the future. How it will be used, how it will develop, and who will be using it.

In this chapter, we'll try to address these questions, talking less about the buzz you hear about, such as illegal activity, but rather focusing on the future of the positive and practical aspects, such as online markets, and, more importantly, privacy. For the future of the Dark Web is intrinsically entwined with the future of privacy for all of us.

So let's go...back to the future!

We will cover the following topics in this chapter:

- What does the future of the Deep Web hold for us
- Dark Web markets
- The TOR Project
- Public interest in the Dark Web

What does the future of the Deep Web hold for us?

To contemplate the future of the Dark Web, we need to also discuss the Deep Web, since they are intrinsically related. As I explained in `Chapter 1`, *Understanding the Deep and Dark Web*, the Dark Web is a sub-section of the Deep Web. The future is almost always unclear, especially regarding technology, which progresses in leaps and bounds, and is usually, not in a linear fashion.

If you remember, the Deep Web's difference from the Surface (WWW) Web is the fact that the sites and content there aren't crawled or indexed, so won't be accessible via standard search browsers.

Organizational content and intranets are part of the Deep Web, but more and more of them are being relocated from on-premise solutions, to cloud-based environments, such as AWS, Azure, and Google Cloud. There is a concern among users of these technologies that the vendors are collecting information about them.

For example, Google has talked about non-stop collection of data, both private and otherwise. This is probably true regarding all search engines and/or hosting companies, so there will be changes in how organizations and people access the Deep Web.

These changes will include how they authenticate (biometrics, voice, 2FA, and more), how they access the Deep Web, and more.

But, ultimately, many sites, services, and users will change the way they access Deep Web content.

And what about the Dark Web, you might ask?

According to forecasts, the Dark Web will be become more mainstream, yet harder to breach.

The UI of applications designed to access the Dark Web, such as Tor, are becoming more user friendly, helping the mainstream trend.

Dark Web currency

Dark Web currency (that is, Bitcoin, and so on), will grow, with many more cryptocurrencies popping up, which will also be a result (or the cause) of a proliferation of Dark Web access.

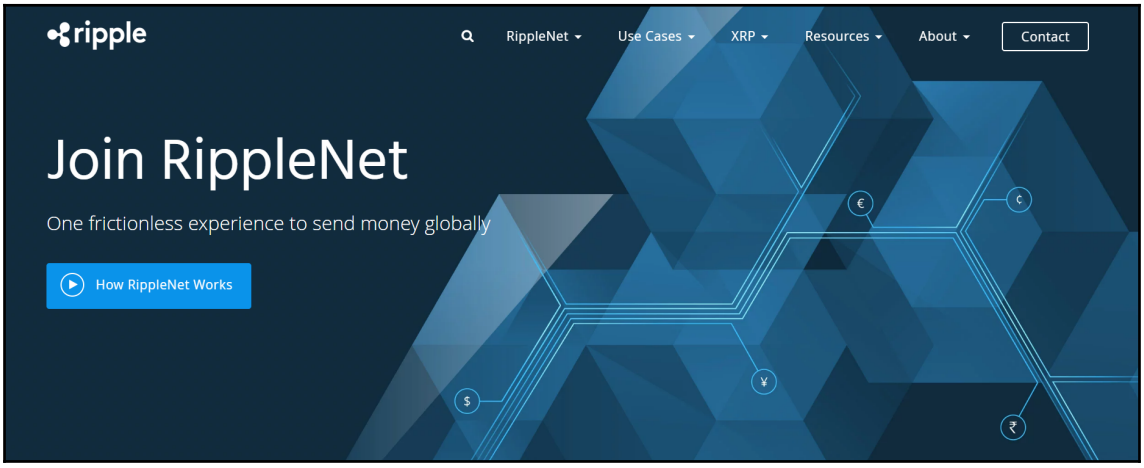
In the future, there will be new, completely decentralized marketplaces that rely on Bitcoin's (or a different cryptocurrency's) blockchain technology. This technology will apparently be used to guarantee trust between buyers and sellers and to ensure safe transactions.

Currently, the top cryptocurrencies are Ripple, Litecoin, Ethereum, Dash, Dogecoin, Banxshares, Stellar, BitShares, Bytecoin, and Nxt, with more popping up all the time.

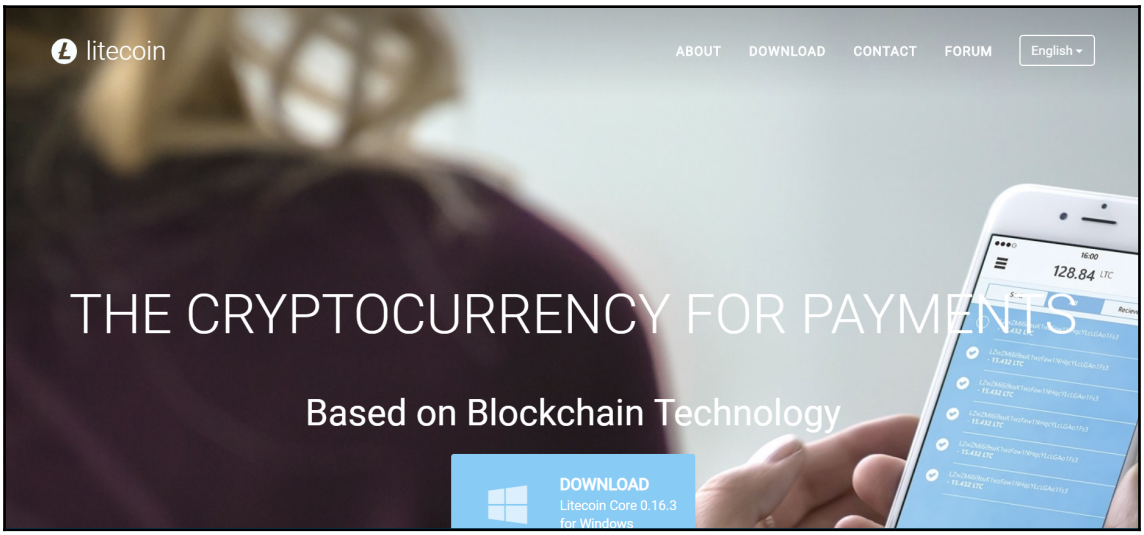
The following screenshots taken from several cryptocurrency websites.

Ethereum is a decentralized platform that runs on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. You could look at it as a secure cryptocurrency platform. Let's look at the following screenshot:

Ripple is a company that provides a secure blockchain-based network, to facilitate secure transactions, called RippleNet. Let's look at the following screenshot:



Litecoin is a peer-to-peer online currency. It's an open source, global payment network that is fully decentralized without any central authorities. Litecoin is a proven medium of commerce complementary to Bitcoin. Let's look at the following screenshot:



Dark Web markets

Since the operations leading to the closing of Dark Web markets, and the ensuing trials, are a matter of public record, many hundreds of people think of new ways to work and create new markets that are harder to bring down.

It's also important to remember that many of these markets sell legitimate goods or services, where the illegal part is usually a lack of taxation on the sale of goods, or a lack of documentation as vendors, and other bureaucratic reasons. Take Dr.X as an example—he provides medical advice, testing of recreational drugs, and support for recreational drug users. There are many countries in the world where this is a legal and positive service.

You can even find vegetables, electronics, and a multitude of other goods that are quite legal to buy and sell.

The original goal of Dark Web markets was to provide free marketplaces, without censorship, where prices are fair and there's no *middle man* between the vendor/seller and the buyer; where the market or the vendor doesn't collect information about us.

Many *regular* market sites advocate information gathering to help with *personalizing* the products offered to us.

Personally, I greatly prefer to search by myself, and not receive offers or have product advertisements sent to me, but nowadays marketing works like that.

The Dark Web markets of the future (and of today, actually) won't collect information about us, unless we allow it. That's just how the Dark Web works.

Think about it: you access a market site, search for what you want, without receiving suggestions or offers, based on your previous purchases, since the market doesn't collect anything about you. I know that I would like that.

Until recently, Dark Web markets came and went. Usually, they were closed by law enforcement, while other times hackers brought them down.

For example, Agora, one of the top markets in 2015, was shut down, due to attempts to crack their security defenses (it is unknown if they shut down themselves or were forced to shut down)

Other markets, such as Hansa and Silk Road Reloaded, expanded their trading onto I2P channels, where they compete with more traditional marketplaces., such as OpenBazaar, a Bitcoin-based market that offers an inventory of goods and services on the Surface Web. Their framework allows for trading directly with customers, using the **Invisible Internet Project** (**I2P**) network, multisig addresses (multisig addresses require multiple keys to authorize a Bitcoin transaction, which allows for dividing up possession of bitcoins), and digital signatures to provide secure communication directly between the buyer and seller.

This is what was displayed on the Hansa site, after it was closed:

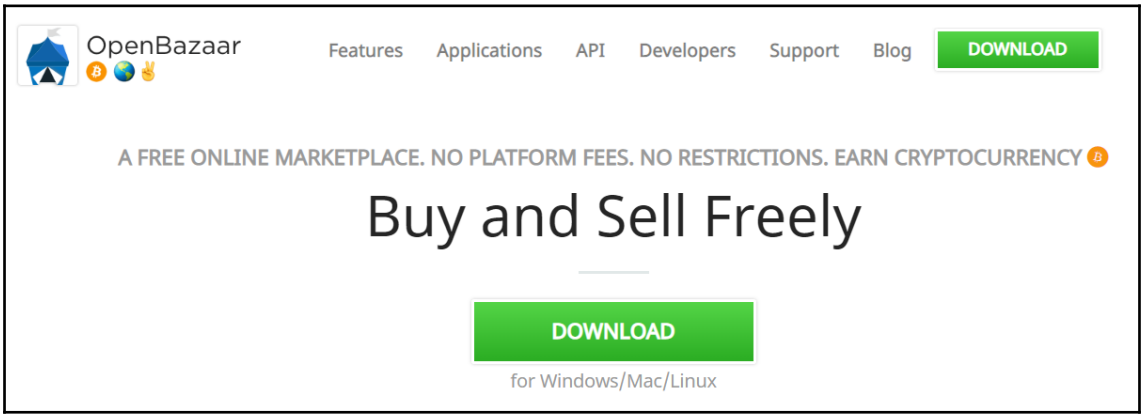
Screenshot of Hansa site

In May 2017, OpenBazaar incorporated a Tor mode option that allows users to become a relay, as part of a Tor network. This will effectively obscure and protect their identity, making OpenBazaar a form of a Dark net site. Since the creators of OpenBazaar view their market as an anonymous one, it is possible for sales of illegal goods to happen, but if this has or will happen, only time will tell.

Anonymous marketplace-based trading will expand and become mainstream in the future. Many questions exist, such as how to resolve differences between anonymous entities (buyer and seller), how to prevent scamming, and more.

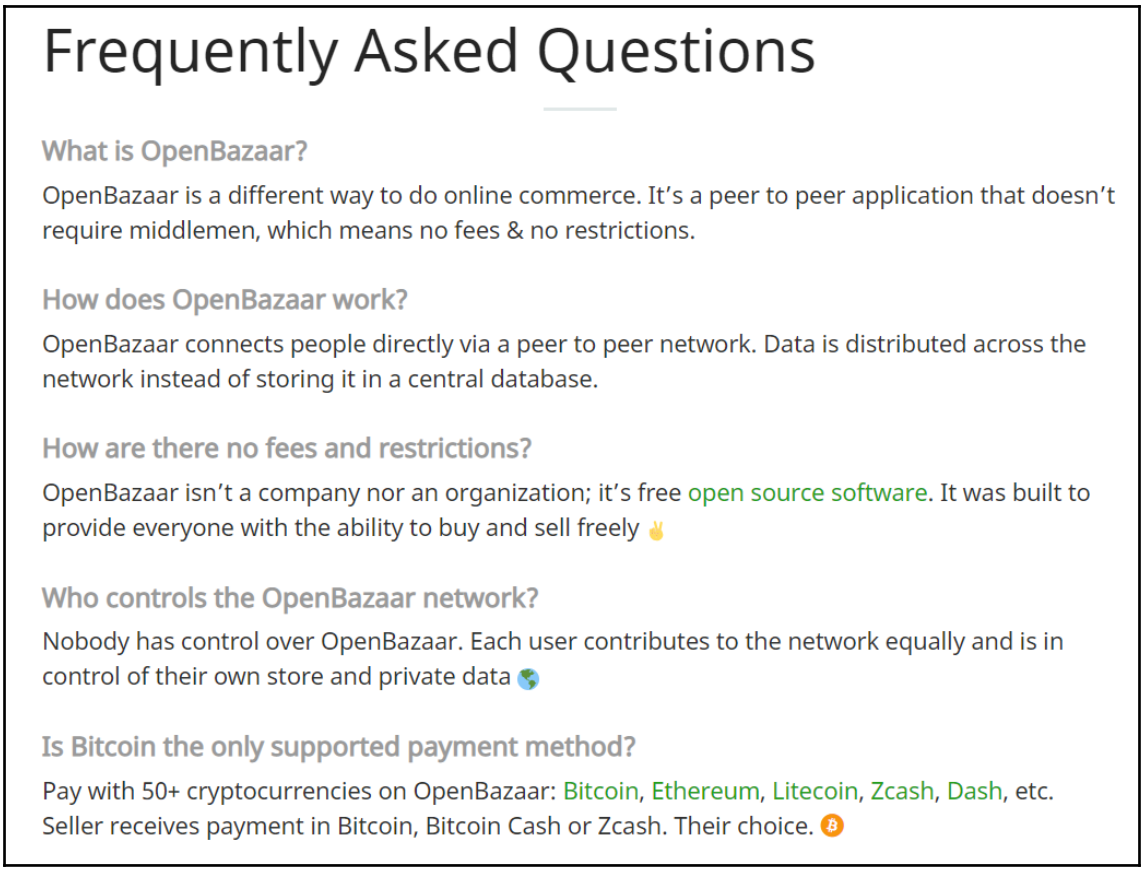
How they will be resolved remains to be seen.

The following screenshot shows the homepage of OpenBazaar:



Homepage of OpenBazaar

The following screenshot displays FAQs from the OpenBazaar site, explaining its concept:



A proposed solution for these Dark Web markets is decentralization. It can help with issues of market operator trust. It provides peer-to-peer sites, written in open source code (more secure), high level of encryption, and privacy.

Centralization is an issue on the Surface Web. Huge companies control large portions of the internet real estate. Take Google, Amazon, and Microsoft, for example. Can we really trust them with our privacy? Let's hope so.

Blockchain behavior should also be implemented into these marketplaces in the future.

One instance where decentralization was tried was Pirate Bay. In 2014, they planned to implement a decentralized version of their site, which would use the resources of the user's machine (buyer or seller). This would ensure continuity of the site, and continue, as long as users accessed it.

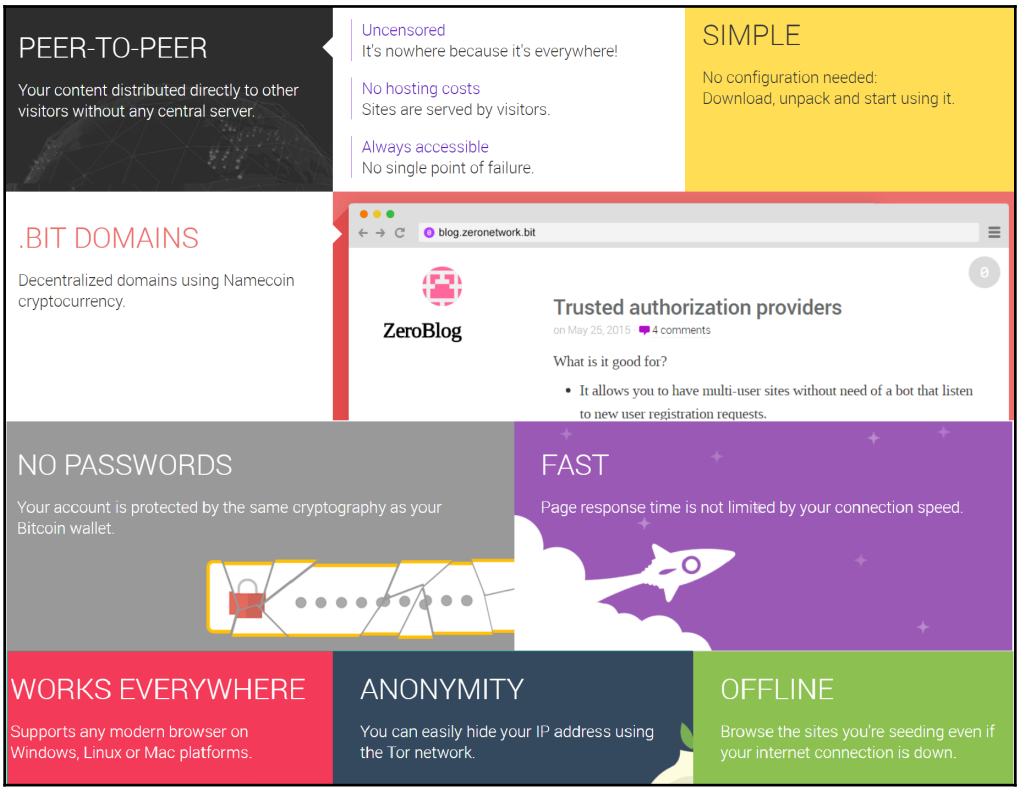
This didn't happen in the end, but the idea was sound, and can be implemented in the future.

ZeroNet:

ZeroNet has created a peer-to-peer system, preventing censorship and hosting costs, without a single point of failure.

ZeroNet removes IP addresses and assigns cryptographic keys to websites, similar to a cryptocurrency wallet address. The public key is the site address, and the private key gives the key holder the ability to create and maintain the site. Users provide the sites to each other, as peers.

The following screenshot of what ZeroNet say about itself is taken from its website:



ZeroBazaar is an example of a new project, a combination of ZeroNet and OpenBazaar, utilizing the best of both technologies, and providing a truly free and private online market.

The TOR Project

As we will discuss in detail in a different chapter, one of the ways to connect to the Dark Web is by using the Tor Browser. It allows a user to connect to the Tor network one of the major Dark nets out there.

As we'll discuss, even without connecting to the Tor network, the Tor Browser provides anonymity and privacy while surfing Surface Web websites.

Due to the rising importance of privacy, the Tor Project is focusing even more on this and on security.

One of the main improvements allows users to host websites anonymously and privately.

Tor's anonymity is based on relays—random computers (also referred to as routers or nodes) between which communication is bounced, to obfuscate the route through which communication is performed, effectively hiding the source and destination addresses, and safeguarding their privacy.

The problem arises from weaknesses (vulnerabilities) inherent in Tor, the same as you may find in any software or technology.

For example, if attackers have control over enough nodes within the Tor network, then they can see both the entry point node and the exit node. They will be able to detect the source of the request and don't need to know what happens in between.

They then modify the headers of the packets in the entry nodes and if they find those packets on the exit nodes they control, they will be able to connect the packets to someone. These types of attacks are called traffic confirmation attacks.

Tor addresses these problems by upgrading the onion services feature.

Onion services allow users to operate a website, chat service, file sharing site, or video-calling platform without exposing their IP address. This feature allows users to run onion services from behind firewalls.

The upgrade will resolve a number of flaws that have existed since the original design of onion services.

For example, in the past, a Tor user was able to set up an onion service manually or by using third-party programs, such as Onionshare. To make the services known, something only the creator could do, he would have to make the services known manually.

Another of those Tor vulnerabilities allows attackers to discover the services, since they had to broadcast their existence to a number of Tor relays.

If an attacker got control of enough relays to identify new onion service registrations, they could develop an index of public and private onion sites, and then replace onion service relays, making the original services unreachable, effectively taking sites offline.

An additional results of the upgrade is that the network will randomly assign the relays that each onion service contacts. The relay message will also be encrypted, making it unreadable to the human operator, but the relay will automatically follow the command.

Also, the onion domain names will include more characters.

Once, they were made up of 16 randomly generated characters. Now they will have 56 random characters.

These improvements should make it much more difficult to discover private (hidden) onion services. And if they are discovered, they require a password. Also, the RSA cryptosystem is being replaced by a more efficient elliptic-curve cryptography.

The hash functions and secret keys for the Advanced Encryption Standard are also upgraded. These improvements are not only aimed at current users, but intend to draw new users to use Tor

Also, as more regular users are using Tor for ethical and legal reasons, the appearance of publicly broadcasted onion services is growing, providing more trustworthy services.

The following screenshot shows the improvements in the latest version of Tor (December 2018):

New Release: Tor Browser 8.0.4

by gk | December 11, 2018

Tor Browser 8.0.4 is now available from the Tor Browser Project page and also from our distribution directory.

Tor Browser 8.0.4 contains updates to Tor (0.3.4.9), OpenSSL (1.0.2q) and other bundle components. Additionally, we backported a number of patches from our alpha series where they got some baking time. The most important ones are

- a defense against protocol handler enumeration which should enhance our fingerprinting resistance,
- enabling Stylo for macOS users by bypassing a reproducibility issue caused by Rust compilation and
- setting back the sandboxing level to 5 on Windows (the Firefox default), after working around some Tor Launcher interference causing a broken Tor Browser experience.

Moreover, we ship an updated donation banner for our year-end donation campaign.

The full changelog since Tor Browser 8.0.3 is:

- All platforms
  - Update Firefox to 60.4.0esr
  - Update Tor to 0.3.4.9
  - Update OpenSSL to 1.0.2q
  - Update Torbutton to 2.0.9
    - Bug 28540: Use new text for 2018 donation banner
    - Bug 28515: Use en-US for english Torbutton strings
    - Translations update
  - Update HTTPS Everywhere to 2018.10.31
  - Update NoScript to 10.2.0
  - Bug 1623: Block protocol handler enumeration (backport of fix for #680300)
  - Bug 25794: Disable pointer events
  - Bug 28608: Disable background HTTP response throttling
  - Bug 28185: Add smallerRichard to Tor Browser
- Windows
  - Bug 26381: about:tor page does not load on first start on Windows
  - Bug 28657: Remove broken FTE bridge from Tor Browser
- OS X
  - Bug 26475: Fix Stylo related reproducibility issue
  - Bug 26263: App icon positioned incorrectly in macOS DMG installer window

Public interest in the Dark Web

The public interest in the Dark Web is growing, especially among *regular* users. These include everyday people like you or me, who aren't criminals, but are extremely interested in the Dark Web, due to the overload of content that we get from the media.

TV shows (*Mr. Robot*, *CSI:Cyber*, *Black Mirror*, to name a few), movies, books, documentaries, and every form of media have been covering the Dark Web in the past few years, and it looks like the trend will only continue.

On the news, we hear about massive hacks (Facebook, British Airways, Ashley Madison, and others) where the data stolen is offered on the Dark Web to the highest bidder.

This image was displayed by British Airways, following their hack:

All these have made even the most technophobic individuals interested in accessing the Dark Web, just to *take a peek* at what they hear about.

As we move forward in this book, you'll realize that there's not that much of a difference between the Surface Web and the Dark Web, except for two main factors—the technological one: the requirement to use specific software to access content there, and the philosophical one—anonymity and privacy abounds there, which simply makes it easier for the criminal elements to perform their activities without revealing who they are.

That's the main reason why illicit activities are more pronounced or readily available for viewing on the Dark Web.
But as we've discussed, and will continue to discuss, taking the proper precautions to protect your anonymity and your security will provide a user experience very similar to what you usually experience on the Surface Web.

Private delivery services will provide untraceable, secure, and anonymous delivery.

One of the things that many people dislike is the way that most regular delivery services invade their privacy. The goal of these delivery companies will be to provide autonomous and anonymous drones, invisible to street-cams, radar, and infrared scanners, delivering packages, payed in cryptocurrency, with no logs of the deliveries.

Yes, this can be used for delivery of illegal products, but one proposed safety mechanism would be detecting bombs or other weapons of mass destruction, and only delivering objects that aren't publicly dangerous. I expect this to be something that will gain focus, since sending such objects, which might result in harm to others, would be a liability to these delivery services, and would harm their reputation and income from the non-criminal market. But, as we are talking about the future, let's wait and see.

One of the problems on the Dark Web is the lack of a justice system. There is no organization that moderates or is supposed to prevent wrong-doing. Of course, there's a very fine line between what's wrong and right on the Dark Web, but it can be agreed that the original intent of the Dark Web is to enhance anonymity and privacy, and not to condone crime. Having said that, many experts agree that actions that harm the privacy and anonymity of an individual or of a business entity should be prevented, in addition to scams and theft, ensuring honest trading (buy/sell anonymously and don't cheat the other side). Sadly, reality is a little different, and people of a less than sterling nature will always try to take advantage of others and do what they want without consideration of morality.

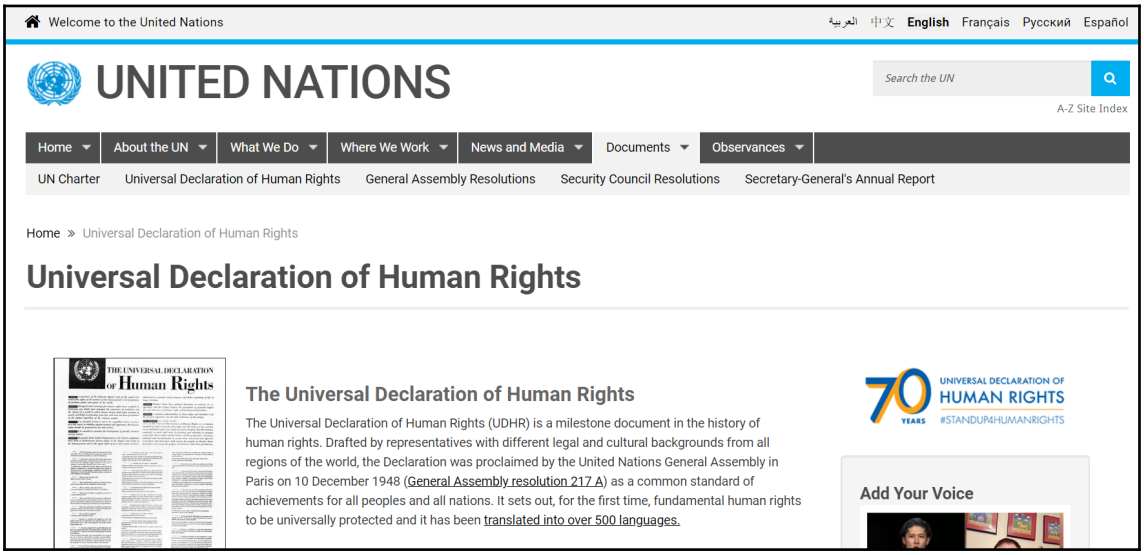
Thankfully, there's an evolution of a Dark Web justice system, which according to the signs, will be a peer justice system, with the majority of users deciding how to resolve conflicts and how to penalize wrong-doers.

Summary

Privacy is becoming more and more important, as there are almost unlimited ways in which information is being collected about us. In some areas, it's regulated in some manner (GDPR in the EU, for example), in others, privacy is non-existent.

The UN has tried to standardize human rights, including the right to privacy (Article 12 of the Universal Declaration of Human Rights).

The following screenshot displays the UN site with the declaration:



The Dark Web is the great equalizer. A way to go online without giving up on our privacy.

It is the beginning of a revolution that will put our privacy at its center.

So in the future, more and more people will use it, to be able to communicate, consume content, purchase or sell goods, and more, with a high level of anonymity.

In the future, the Dark Web will be *the* anonymous communication medium.

Look out for it.

Questions

1. Name three improvements in Tor.
2. Name at least three Dark Web markets.
3. What are the main proposed future changes in the Dark Web?