Digital Forensics and Cybercrime

Gianvito Caleca

2024

Contents

Part I

Cybercrime: threats, modus operandi, underground economy, financially-motivated malware

Chapter 1

Cybercrime: Threat Landscape

Working on security we work on **risk**, which is composed of different elements:

$$Risk = Asset \times Vulnerabilities \times Threats$$

The risk is the statistical and economical evaluation of the exposure to damage because of the presence of vulnerabilities and threats.
With no threats there are no risks, because it is the only thing that can nullify this equation. Assets and vulnerabilities are never absent.
With no *Threat model* we're completely misguided on the management of our system in terms of security.

1.1 Threat landscape

Threats can be roughly divided along three directions:

Internal vs External treaths an internal treath comes from the inside of the organization, it is part of the organization, while an external one don't.

Generic vs Targeted many security threats are generic:

- Generic threats: when you walk towards the underground, you're subjected to pickpocketers: they don't pick you because it's you, you're one of the others, it is a generic treath.
  Generic threats are not linked to us by definition, they are linked to us because we look alike somebody easy to be pickpocketed, not because we were the target.
- We can also consider also threats which are not so very generic: aggressions for sexual reasons are more targeted to one gender than one other, while still being generic.

- Targeted threats: specifically designed against us: criminals target **that specific company** *(e.g. the know how for racing cars, i want to steal from THAT company in particular).*

These directions also affect the kind of attacker: pickpocketers vs highly "professional" skilled stealer of information

Financially motivated vs Anything Else we divide:

- **financial attackers** *(which are the most of them)*,
- **other attackers** *(governments, secret services, hacktivists..)*.

Financially motivated attackers has 2 important positive characteristics:

- **easy to predict:** you look at valuable goods from companies and you can predict who the attackers can be *(e.g. ransomwares)*
- **they're relatively easy to handle:** just deny them the opportunity to take money, like making it too costly wrt what they want to earn.
  Notice that what is easy to understand is how to handle them, not to actually handle.

Non financially motivated ones are more difficult to handle:

- We cannot make them too costly or too risky *(e.g. Russians vs Ukraine's Donbass power plant: they have an entire state funding them, and they cannot be arrested for it)*, they have more money and they can take more risks
- If they're internal, they already know about the company and its security systems.
- The more motivated is the attack, the more determinated is the attacker

1.1.1 A gartner quadrant of threats

	Generic	Specific
Internal	**disgruntled**[1] employee	**socially-engineered or disonhest** employee *(financially motivated)*
External	Criminals, usually looking to make money *(financially motivated)*	A variety of advanced hackers *(mostly financially motivated)*

- **Generic internal threats:** a disgruntled employee who wants a raise, has something against his colleagues, was fired ...
  The treath doesn't need to be linked on what the organization does.
- **Specific internal attacks:** former employee stealing from old employer and bringing to the new one, it also exists a specific job which consists in being hired from companies just to steal from them.
  Or, employee can also be *social-engineered* into behaving like attackers.
- **Generic external attackers:** attackers which want to earn quick money, they aim to things which are common for all companies, like stealing money from bank accounts and so ....
  They are mostly motivated by financial reasons.
- **Specific external attackers:** industrial spies which aim for money, or governments or terrorists aiming for the destruction of a power plant near Donetsk.

The most important quadrant is than the one which comprends disonhest or social engineered people *(human factor)*: our instinct say us that we need to protect from the outside because we are clan-based animals, and we have our group of trustworthy animals *(our clan)* to which we are positively implicitly biased. **Think about the most famous security technologies:**

- Firewalls are meant to keep people out
- Antiviruses are meant for generic attacks, they use a generic list of malwares

Most of our security technologies protect against external attackers.

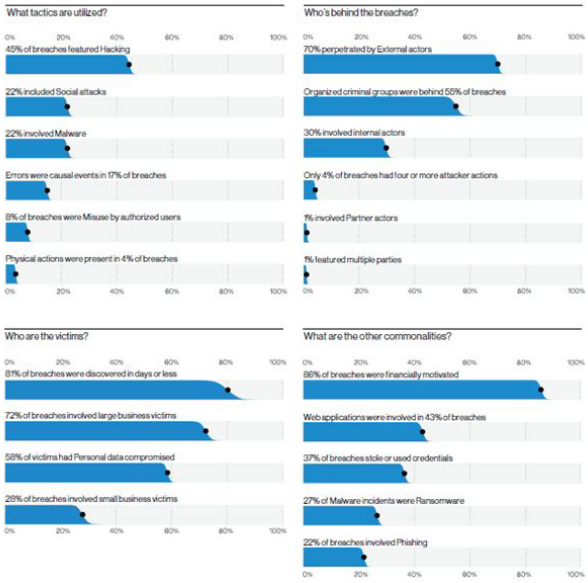
1.1.2 Examples of internal treaths

A bit more on:

- **Reckless or socially engineered employees:** in security we often have a wrong perception of the *human element*.
  When a company gets infected by a malware because a user clicked on a link or something similar, we blame the *stupid* user for it. But, actually it's not fault of the employee: it is fault of who had the responsibility to manage the fact that a threat was present and it had to be controlled.
  Since there will always be someone to click on links, our job is to make sure that they doing it doesn't cause damages to the organization.
  e.g. in aviation they study human factor to understand what to do to don't let people make mistakes: in airplanes cockpits there are different levers with different shapes, them are exactly shaped the same in different kinds of planes, it is a standard, and the reason is because people lost their lives because of similar levers.
  The solution wasn't to train pilots, but to make the threat difficult to happen.

- **Thirty-party users:** they're for example consultants that work in a company for a long time, where they actually do jobs very similar to the ones of the actual employees while not being true employees of the company.

1.1.3 Data breaches and targeted attacks



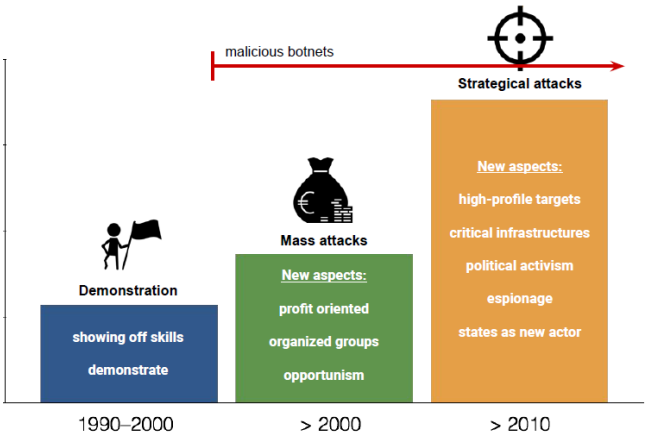
Verizon has a big sample of incidents made to their customers:

- The largest part of the attacks features hacking of some sort, the second larger chunk comprends social attacks.
- The 70% of breaches are perpetrated by external actors. This means that 30% of them starts from the inside, an incredibly high percentage.
  Consider that data are skewed[2], in the real world the internal attacks can be even more! *(remember the external threats reasoning, rationality (data) tells us that a lot of threats come from the inside, while our instinct guide us to be aware of the outside)*
- The 86% of them were financially motivated, 14% which are not, are a lot too!

These data are biased and are not representative of the true reality of threats, because simply they're not all collected. This collection can still help us to rationally think on how to manage the overall situation.
Keep in mind that some security incidents are specifically designed to be difficultly found, a lot of them has never been. This means that there is an entire set of breaches that no one ever investigated.
We measure attacks that we investigated/detected, and this is called the **observation bias**:
Other attacks by their nature be discovered, *(e.g. Dos, ransomware . . .)* that's the reason why they are so prevalent in our statistics: they are observed.

[2] biased

1.2 Brief history of malicious software



Over the last few decades attacks and attackers changed:

- **1990-2000:** most of the attacks were meant to show skills and explore
- **2000-2010:** with the birth of the Internet, massive, profit oriented attacks born. In this period were born also groups working as profitable enterprises of cybercrime.
- **2010-today:** attacks evolved: mass attacks kept happening, but now a lot of them are high profile financial attacks *(before: ransomwares, i ask small amount of money to single persons. now: ransomware attack specific companies to get a lot of money)*

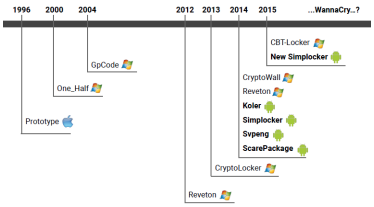
1.3 Financially motivated attackers

Today financially motivated attackers are the "mass", they're interested in monetizing their attacks in possibly two ways:

- **Direct Monetization:**
  - Credit card/bank account frauds
  - Ransomware attacks
  - Crypto-miners
  - Fake antiviruses: they show you warnings that say your computer is infected, and to pay to activate the premium version to get rid of the malware. In reality they are just fake programs asking you to pay for a license.
  - Premium calls: back in the days when you called to connect to the provider, someone managed to change the number to let you call a costly one.
- **Indirect Monetization:**
  - Abuse of computing resources
  - Information gathering (stealing of account infos to sell them)
  - Making the machines part of a botnet to rent or sell the botnet

1.4 Direct monetization: ransomware attacks

1.4.1 Brief history of ransomware



In 1996, a paper describing a crypto-malware that was exactly a ransomware was published about 15 years before CryptoLocker which was the first really successful one.
They just *"looked into the crystal ball"* of what in the future would be valuable: taking as hostage digital valuables could become a good way to steal money.
Then something happened:
the internet in 1996 was really different than the one of 2013, ransomwares needed a way for the user to pay a ransom in a way that was easy to perform. The preferred way to perform payments on internet is with credit cards, but this kind of payments have two important difects:

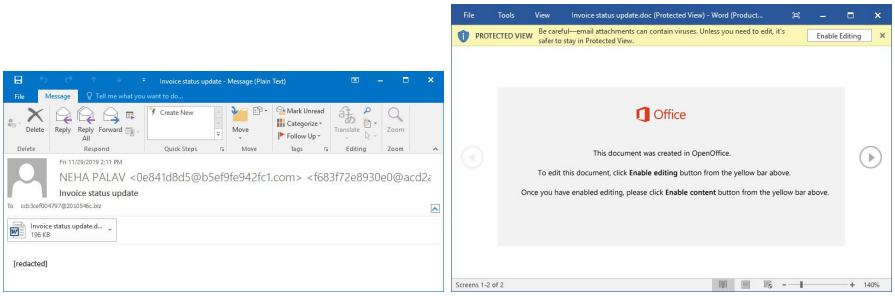
- they are trackable
- they are refundable when fraudolent

Then a new suitable way for payments was born: **cryptocurrencies**.
They perfectly fit this need: they are easily accessible, and payments are not reversible.

1.4.2 Ransomware screenshot and social meanings

Look at the structure of the timer: it is made to let you to percieve urgency. The stress of the urgency makes human take bad decisions, with the timer running you're more prone to pay because you feel that you have limited time. In social engineering attacks, urgency is always an important part. *(think about ultimatums in diplomacy, job offers with time limits, poltrone e sofà...)*

1.4.3 How to get infected



(a) (b)

Looking at the images we can see an interesting example:

- User receives an e-mail with a short text that contains some sensitive information and an attachment which is social engineered in a way that many people would click
- Microsoft Office shows a message to try to prevent code execution, but the user is prone to click "Enable" because the text contained in the document makes him think that's the right thing to do, even if a lot of grammar errors are present and the whole situation looks suspicious

One could have said that the user must had to be trained to not click, but the reality is that he is not understanding what's happening on his computer.
We can't train a generic user to not click: if your job is to open invoices received by e-mail, there is no way you can be trained.
Even if we train him to click only on what is coming from attendible e-mail addresses, if the *"attendible"* part was hijacked?
What we really should do is to figure out a way that when someone clicks enable, this won't cause any damage. Of course, to train the user to let this happen the less frequent possible is good, but not the main thing to do.

1.4.4 Encryption mechanism: how do ransomware work

Once the malware starts running on target computer, it generates a random symmetric key[3], usually one per file, and it encrypts each file with it.
The symmetric key itself it's encrypted with a public key, of an asymmetric key pair generated on the server of the group that runs the malware. The private key is stored on the server, and it will released only when the ransom is payed.
Most of this process is automated: when cryptocurrencies are transferred to the criminals' address, the server releases the key associated to it. Different keys to allow the attackers to decrypt only a part of the samples to demonstrate that they can do it.

[3] used both to encrypt and decrypt information

1.5 Indirect monetization: Botnets

The word botnet comes from the words *robot* and *network*. A botnet is composed by few hundreds to millions of infected devices which run some sort of malware they got by opening an infected email attachment, by plugging an infected USB drive, visiting an infected website *(these are examples of ways to get infected)*
Each botnet has a **botmaster** who controls and rents it out to perform tasks *(denial of service, spamming, phishing campaigns, crypto mining . . .)*, and his only objective is to earn money by renting them.
The significant challenge with this type of crime is that each bot per-se is not dangerous for the machine itself, but for other machines, and since the cost of cleaning up a machine falls on its owner, some can decide to not do anything about. This cost can be seen as a small fee to be payed by *the community* to get everybody safe. Like a vaccination, some cases of infected machines are not a big trouble for the community, while a lot of them can be really dangerous for everybody.

1.5.1 Rise of the bots

Back in the days botnets were used to control IRC chats *(see IRC wars)*. Then instead of using the compromised machines to control the chat, botmasters started to use the chat to control the bots.
In 1999, there was one of the first DDoS attacks, which was against University of Minnesota and used at least 227 bots.
In the 2000s DDoS attacks against high profile websites *(Amazon, CNN, eBay . . .)* got huge media coverage.

1.5.2 Geolocalization of botnets command and control

Rank	Country	Q2 2020	% Change Q on Q
#1	United States	896	7%
#2	Russia	812	32%
#3	Netherlands	337	61%
#4	Germany	185	7%
#5	Singapore	131	157%
#6	France	108	35%
#7	Great Britain	89	37%
#8	China	74	-15%
#9	Bulgaria	72	38%
#10	Hungary	70	New Entry

This chart shows the number of new botnet C&Cs detected by *Spamhaus* in the second quarter of 2020, and the increase wrt the first one.
By keeping in mind the *observation bias*, we can also introduce another kind of bias which is called **heatmap effect**: we're biased on the density of the population and on how much data we collect from a certain country.
In this kind of charts we'll always have U.S.A. on top, because there's more penetration in the internet, and also this kind of things is tracked. While we'll have less data from less technological advanced states or *perfectly democratic countries* like Russia or the P.R.C. which can result in lower positions while in reality being the first ones.
Here we see an important increase of C&C from The Netherlands:

- it is possible that **something is on**
- or simply that some Netherlands organization decided to participate in this data collection feeding a lot of *new* data

Funny thing about Russia and P.R.C: Russian people hack russian computers too, while P.R.C citizens don't hack into their fellows machines.

1.5.3 Type of (botnet) malware families

Rank	Q2 2020	% Change Q on Q	Malware Family	Description
#1	436	772%	AgentTesla	Credential Stealer
#2	290	-46%	Lokibot	Credential Stealer
#3	169	New entry	RedLineStealer	Credential Stealer
#4	156	51%	NanoCore RAT	Remote Access Tool (RAT)
#5	112	-27%	Gozi	e-banking Trojan
#6	98	-5%	AZORult	Credential Stealer
#7	92	1%	RemcosRAT	Remote Access Tool (RAT)
#8	74	23%	njrat	Remote Access Tool (RAT)
#9	74	New entry	DanaBot	Credential Stealer
#10	69	17%	ArkeiStealer	Credential Stealer
#11	67	63%	KPOTStealer	Credential Stealer
#12	62	New entry	IcedID	e-banking Trojan
#13	61	New entry	AveMaria	Remote Access Tool (RAT)
#14	55	-18%	Adwind	Remote Access Tool (RAT)
#15	51	21%	NetWire	Remote Access Tool (RAT)
#16	47	New entry	QNodeService	Remote Access Tool (RAT)
#17	47	57%	RaccoonStealer	Credential Stealer
#18	46	-4%	Pony	Credential Stealer
#19	45	105%	AsyncRAT	Remote Access Tool (RAT)
#20	43	New entry	Zloader	Loader

Every botnet in general can be used to do any sort of things, but they're used to do only one of them:

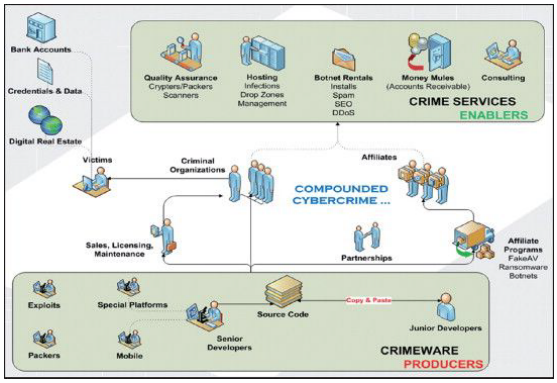
- **Credential Stealers:** used to steal sensitive credentials.
- **Banking Trojans:** credential stealers specifically designed to perform stealing of bank accounts information. *(Gozi is the most common one, Zeus the most important one)*
- **Remote Access Tools:** basic botnet oriented malware, which allows to control a computer in order to perform whatever.
- **Loaders:** specifically designed to allow a botmaster to load a program of whatever sort on a computer. Maybe a client ask you to install a certain malware on a lot of computers, and you can do it with a loader.

We talk about families because there are criminal groups that only develop their source code, and who performs the attacks buys the code and personalizes it for the specific purpose they need.
So we can consider three businesses: how to develop them, how to configure them, how to use them.
There is a market for services related to malwares and cyber attacks *(cybercrime as a service, underground market...)* structured around the needs of cyber criminals. This market is fueled by the money that these schemes make. Some of these money pays for the tools used to make that money.

1.6 The cybercrime ecosystem

The status quo consists in **organized groups** performing **various activities:**

- Development and procurement of exploits
- Site infection
- Victim monitoring
- Selling *exploit kits*



These ecosystems can exists because some of the activites done are not illegal: developing exploits per-se is not illegal, selling one is not illegal, the usage of them may be or may be not illegal. Even the services related to the configuration of malware are not illegal, while execution and operation may be. If you're sufficiently shielded and you run these *businesses* in countries that cannot persecute you, we can even know your name and surname but you cannot be arrested.

- Developers write the source code for malwares with the help of packers and exploits developers
- Crime service enablers:
  - Quality assurance makes sure that antiviruses don't detect their software
  - Bulletproof hosting is a kind of *close-an-eye* hosting, *(e.g. russina business networks)* with permit certain suspect activities over their infrastructure, they're sort of borderline organization with lot of regular customers, and some bad ones

1.6.1 Identity sales

People's identities are sold on the black market. They are worth because they can be used for fraud, to open bank accounts used for money laudering for example. The more they're useful, the more they are worth. Worth 50 dollars for you that sell it, the one who pays is going to use them for fraud which is worth more. The black market is fueled from an enormous amount of money that people stole.

1.6.2 Drive by download

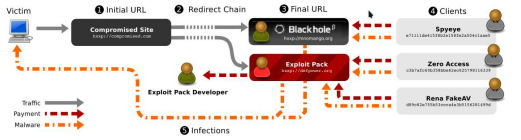


Figure 1: The drive-by-download infection chain. Within the exploit-as-a-service ecosystem, two roles have appeared: *exploit kits* that aid miscreants in compromising browsers (❸), and *Traffic-PPI* markets that sell installs to clients (❹) while managing all aspects of a successful exploit (❶,❷,❸).

This is another way in which malwares are installed:
an exploit breaks into your browser and executes code on your machine. This requires your browser to be vulnerable and for you to visit a compromised website with the exploit running *(streaming, cracks of programs websites,...)*.
The most compromised are *factually illegal websites*: you're not scared of the strange url if you are in need to see the last movie in streaming, download the expensive program's crack, this is in contrast with a normal situation like going to amazon to buy shoes.
But, *traps* can be also present in legitimate websites.
What actually happens is that the users endup in a series of redirects, called **redirect chain**, which will endup in a visit to a website running what is called **exploitation pack** for your browser.

1.6.3 Exploitation kits sales

This kind of kits is sold in the dark web by well known organizations, take *Blackhole* as example:
they were buying exploits from developers to earn 10s of millions per month renting them.
Their boss, surprisingly called Dmitry "Paunch" Fedotov, was arrested in 2013 after years of running the website.

1.6.4 Monetization on the dark web

Monetization takes a lot of forms, one of them is stealing credit card numbers to sell them for a relatively small price.
The hackers get *easy and fast* money, while the buyers need to use the real

money on the cards to buy expensive objects or to start frauds because they can be easily refunded. *(apple computers, ethnic travel example..).*

1.6.5 Cybercrime and perception

Online, you detach people from the picture. It's actually easier to commit crimes, it's easier to crack a program instead of stealing a car, lot of cyber criminals would never be criminals in the real world. But when you do cybercrime, your perspective is different: you have another perception of what you're doing, that's the reason because crime happens more online.
Ethical people understand the consequences of their actions, and may decide to not do them, but someone can not care about what can happen as a consequence of their actions and perform them anyways:
in the Jamal Khashoggi case, the exploiter which wrote the code for the spyware that ended up to make him killed, would never kill someone. But the consequences of his actions did.

1.6.6 Money mules and money laundering

Most cybercrimes end up with a digital form of money, which crimials want to bring in a physiscal form, completely disconnected from what they did in principle.

- They can pay invoices to companies somewhere in the world, which in a certain way makes sure that the money come back clean. *(traditional way)*
- They can make use of **money mules**

Money mules are intermediary people which by purpose or not make earnings coming from cybercrime clean money.
Accomplished ones may be people that have nothing to lose *(prejudiced, poor people . . .)*, they just open bank accounts by their names and get the money transferred and then withdrawn and handed to criminals.
Some of them may also open accounts by somebody else's name using identities that may be stolen with an attack and bought online. They're most difficult to catch because the Police needs to be actually there while they are withdrawing money.
Unaccomplished ones may be people which are fooled by things like the Nigerian prince scam: they get the money on their bank account, send 70% of them to criminals in packages or by moneytransfer, and keep 30%. Most of the cases they get arrested and have to pay back all the money, also the ones they don't own no more.
Buying and selling of goods *(ricettazione)*, videogames curriencies, . . . , are other ways to perform money laundering.

Chapter 2

Cryptocurrencies: abuses and forensics

We talk about cryptocurrencies in the way they are used in cybercrime.

2.1 Bitcoin and blockchain

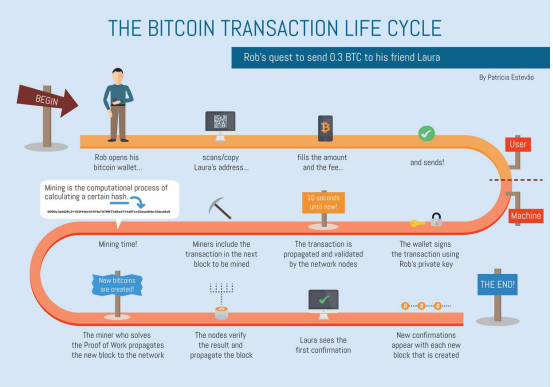
Bitcoin is an attempt to create **electronic cash**: a digital currency that has lots of properties that physical money have, one of them is **no central authority**. What Satoshi Nakamoto wanted to have is an electronic distributed ledger[1].
Having no central authority is a really hard problem to solve *(byzantine consensus)*, he did it with **the blockchain**.
The blockchain is a **shared, append-only, trustable** ledger of all coins transactions. The limits of distributed consensus defined in the Byzantine Problem and CAP Theorem are solved using the technique of **proof-of-work**.

2.2 Wallet and addresses

A wallet is the software that allows to manage and store the **public** and **private** keys for each of the user's bitcoin addresses. To create and sign transactions, track the balance.
A bitcoin address is an alphanumeric string which identifies a *point* where you can send bitcoin to, and where they can be sent from. In order to know how many Bitcoin are *stored* in that key you need to go to the origin of all the transactions and track the flow of them to understand how much of them are there now. This computations is not really efficient but can run without central authority, so the only reason for using a blockchain is if it is really so important to get a way out of a central authority.

[1] ledger=registro

2.3 The bitcoin transaction life cycle

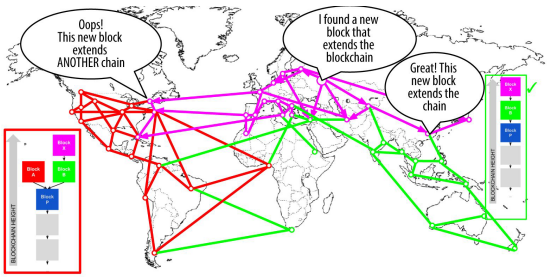


As soon as the transaction is on the immutable ledger, the money are on the other address. How do we ensure that this is the only transaction done with those Bitcoins?
Our immutable ledger must be consolidated, with a central authority that would have been easy, how do we agree with no central authority? We need a history that cannot be modified, and to do this we talk about mining.
Mining is the process to generate a block containing all the transactions, and to append it to the blockchain.

2.4 Mining

Miners compete to generate a new valid block that solves a complex mathematical problem bybruteforce: the solver is then rewarded a fixed number of BTC. It is a computational demanding activity: miners put a set of transactions in the new block, put there a destination for the reward and then start bruteforcing the block to find a sha256 hash of it which starts **with a certain number of zeros**. The more zeros, the more difficult is the process.
When a block is added to the blockchain, the other miners stop bruteforcing their blocks and start to compute the hash of another one, to link it to the last found block. The difficulty increases more and more, the reward got smaller and smaller but BTC value gets larger and larger.
Besides of the reward you get, you can also put a fee you want to receive from the transactions you included in the block. Since reward is becoming smaller, fees are becoming larger. Now the fees make small transactions unfeasible.

2.5 Fork events



Sooner or later two miners will get a solution at more or less the same time. This causes a fork where the situation is that for some miners the blockchain ends with block A and for some others with block B.
Now the blockchains are two, and sooner or later some miner will find a solution and append a new block in one of them. The rule says that **the longest blockchain is the true one**. As soon as one blockchain becomes longer, all the miners move to that leaving the other one sadly alone.
This is done because in order to revert a payment you'd need to go back on your block, go ahead mining until your blockchain is the longest one: this means that you would compete with all the other miners. To be sure that a certain transaction is there and cannot be canceled, you must wait that the block in which it finds itself is a couple blocks behind the last one.

Part II

Fraud detection and analysis

Part III

Digital Forensics principles

Part IV

Acquisition, analysis, evaluation and presentation of evidence

Part V

Ethics elements

Part VI

Optional: casi studio specifici