Information System Security

Dark Web

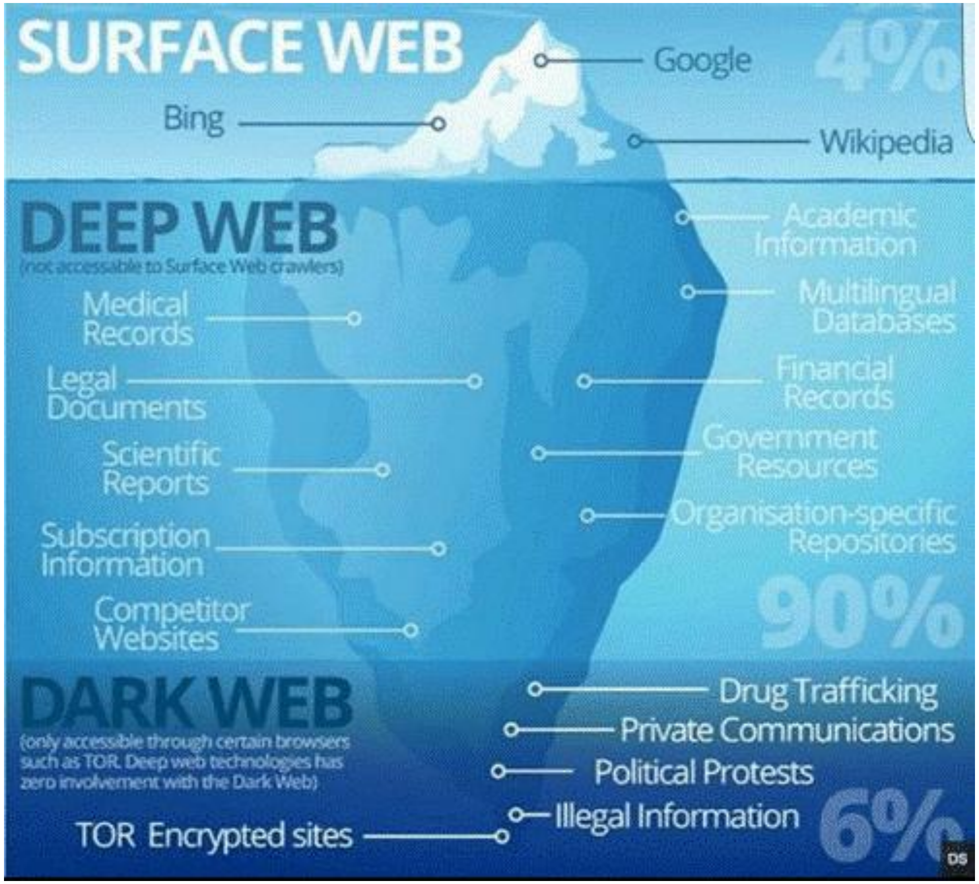
ECE PARIS
ÉCOLE D'INGÉNIEURS

Summary

- Web, Deepweb, Darkweb, Darknet
- Tor
- Hidden services
- Blockchain
- Bitcoin

Web, Deepweb, Darkweb, Darknet

- **Web**
  - Accessible from known browsers
  - Is a set of pages linked by hypertext links
  - 47 billion pages indexed in August 2018 (source : http://www.worldwidewebsize.com/)
  - Public Internet websites only represent 4% of all information on the Web



Web, Deepweb, Darkweb, Darknet

- **Deepweb**
  - Set of pages that can be :
    - ✓ Bad or not referenced by web search engines
    - ✓ Protected by authentication
    - ✓ Incomprehensible for web browsers
  - **Any site may have content in the "Deepweb"** most of which is restricted access (bank account, cloud, webmails and all kinds of private space)
  - The Deepweb is estimated at 14 trillion (14,000,000,000,000) pages and if we speak in storage unit some zettabytes (10^{21} bytes)

Web, Deepweb, Darkweb, Darknet

Darknet

- You can’t find a page of Darkweb via your conventional browser, it is necessary to use specific tools…
  - ✓ To access it you need a special "browser" such as TOR Browser, Freenet or SafetyGate Invisible
- .fr .com .org extensions do not exist in the darknet
- Its pages do not use the same protocols as the classic internet
- Although it represents only 6% of the entire Web it remains more than the indexed part
- Originally created for political dissidents in countries where human rights are violated
  - ✓ There is a lot of political content: blogs, news websites run by journalists, libraries

Web, Deepweb, Darkweb, Darknet

Darknet

- There is no search bar, you must know the address of the site you are looking for

- Serves as a haven for hackers
  - ✓ They host **blogs, forums or wiki**
  - ✓ They share tips and snippets of **code**, they exchange **software** made by them or services of development
  - ✓ These services are exchanged with **crypto-currencies**
- But the majority of this part of the web remains **illegal**: sale of drugs, weapon, human, child pornography, hacking forum, stolen software codes, stolen identities, etc

TOR

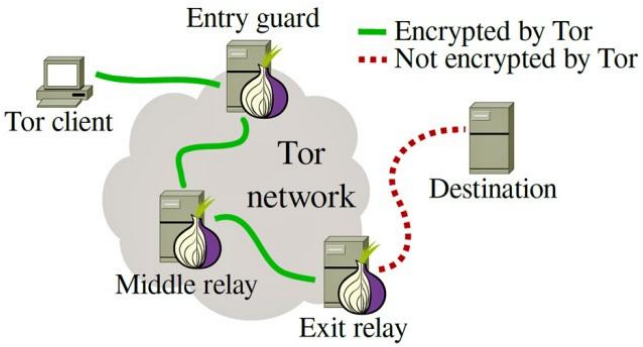
- **Tor (The Onion Router) is a network of proxy servers**
  - Communications are routed randomly through a network of independent proxies
  - All traffic between Tor servers (or relays) is encrypted
  - Each of the relays knows only the IP address of two other relays, the one that precedes it immediately and the one that comes immediately after in the chain

TorProject.org

- **It becomes very difficult for:**
  - The ISP to know who we communicate with and what information we send
  - The target website to know our IP address
  - One of the independent relays to know who we are and with whom we communicate
- **Tor offers far more anonymity protection than a single proxy**

How Tor works

- **Construction of the circuit (choice of relays to create a random path)**
  - ➢ Retrieving the public key of each node
  - ➢ Encrypting the package as many times as nodes in the path starting with the output node



- **Each node decodes a portion of the envelope and forwards the data to the next relay until it reaches the exit node**

- **Only the output node knows the original package and sends the request to the actual destination**

- **A relay is not able to trace the complete path of a packet that would reach him**

Tor risks

- **Tor is vulnerable to blocking**

  - Tor nodes are listed in a public directory
  - It is easy for network operators to access this list and add node IP addresses to a filter

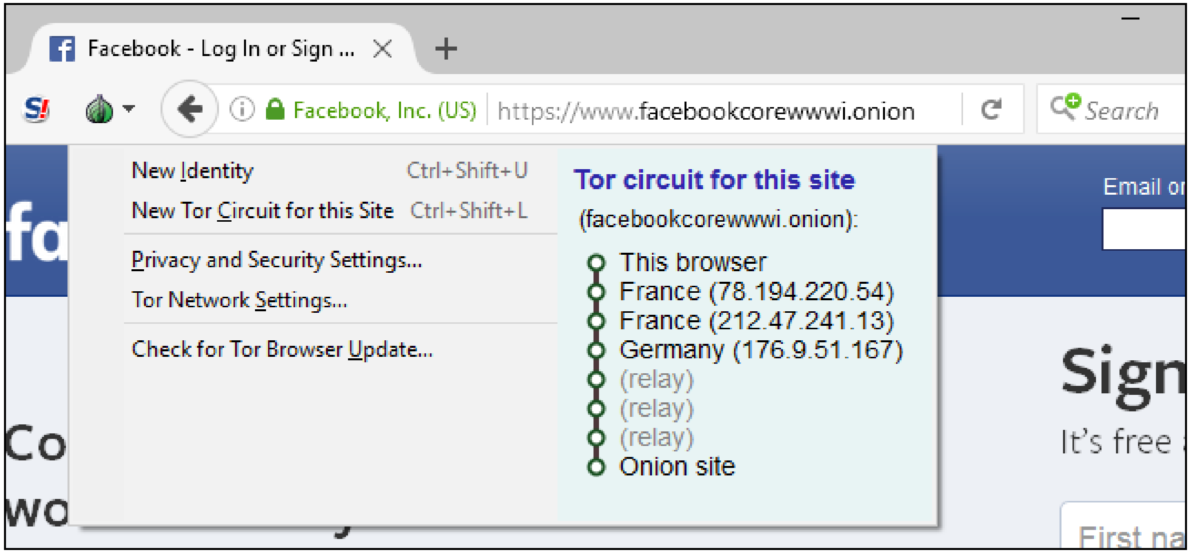
- **Some programs have problems that can compromise anonymity**
  - Running scripts on the client machine (Flash, JS ...)
  - Saving cookies or other information on the client computer

- **Data is decrypted at the output node**
  - If there is no additional encryption (HTTPS), the data is visible by the owner of the last Tor node and by the ISP between this node and the destination

- **Ability to break anonymity if an entity has a large portion of the input and output nodes**
  - Correlation of network traffic exchange frequencies between input and output

Hidden services

- **Tor can offer services while hiding its location**
  - Using the principle of “rendezvous points", users can connect to these services while maintaining the network anonymity of both parties
  - An onion service must announce its existence on the Tor network to be contacted
    - ✓ The service selects relays to serve as a point of introduction and communicates to them its public key

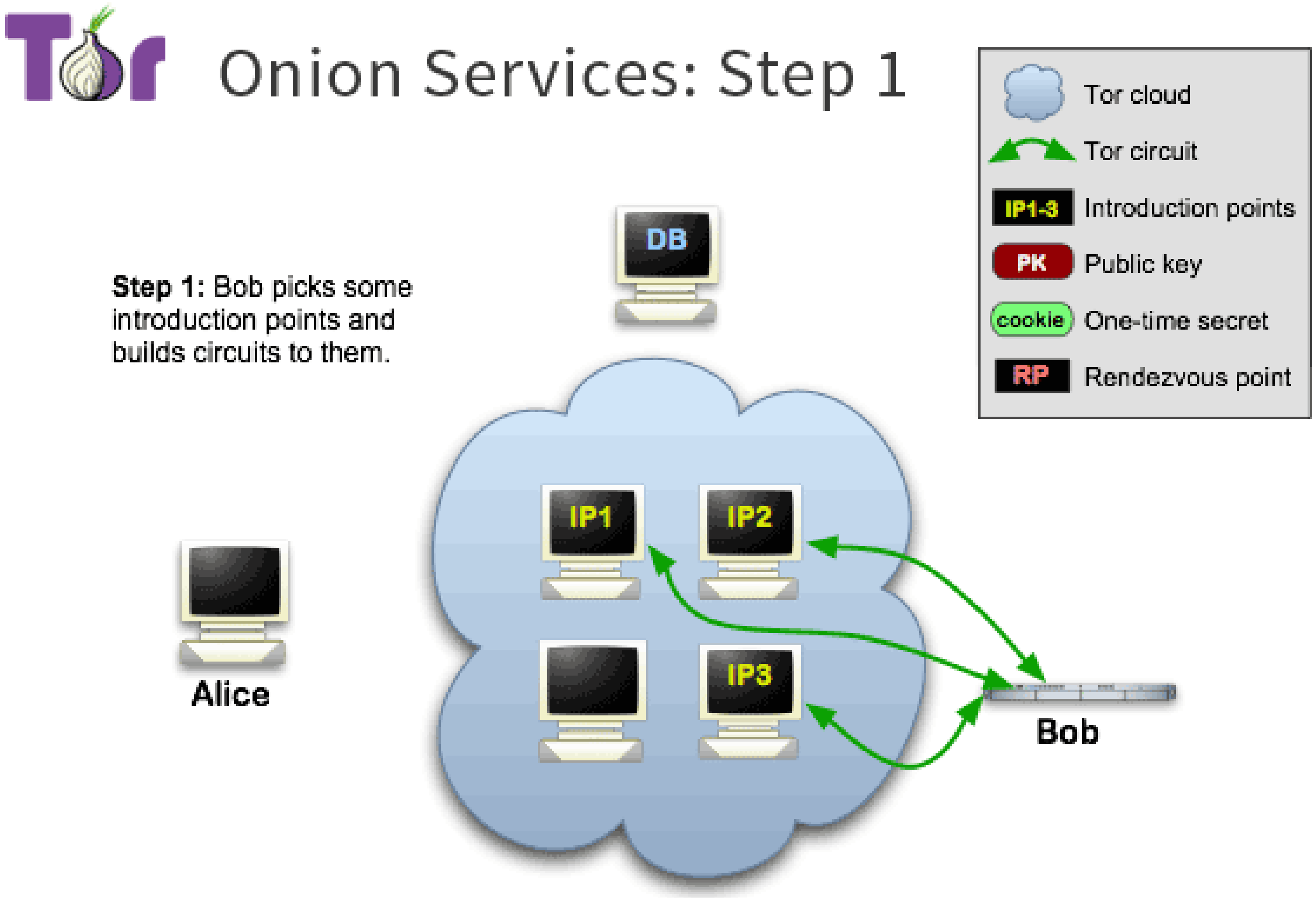

Facebook - Log In or Sign ...
Facebook, Inc. (US)
Search
New Identity Ctrl+Shift+U
New Tor Circuit for this Site Ctrl+Shift+L
Privacy and Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
Email or
Sign
It's free
First na

https://www.facebookcorewwwi.onion

Tor circuit for this site
(facebookcorewwwi.onion):

This browser
France (78.194.220.54)
France (212.47.241.13)
Germany (176.9.51.167)
(relay)
(relay)
(relay)
Onion site

Hidden services



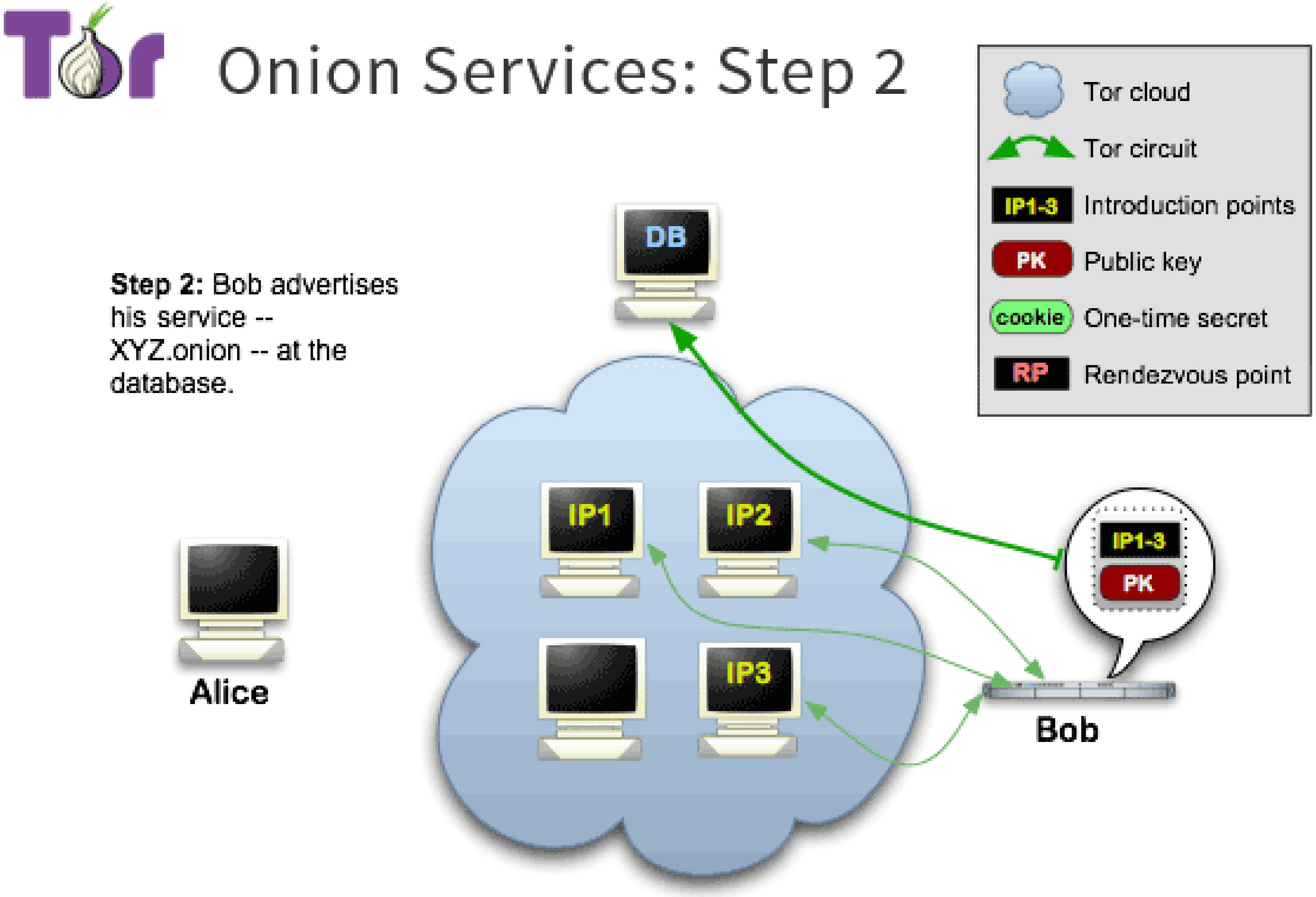
Onion Services: Step 1

Step 1: Bob picks some introduction points and builds circuits to them.

Hidden services

- **The service creates a service descriptor containing**
  - Its public key
  - A summary of each introductory point
  - Signature of the descriptor with its private key
- **This descriptor is inserted into a distributed hash table**
- **The descriptor will be found by customers requesting XYZ.onion**
  - XYZ is a 16-character name derived from the public key of the service
  - Benefit: everyone (introductory points, hash directory and clients) can check that it speaks to the right service

Hidden services



Tor Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.

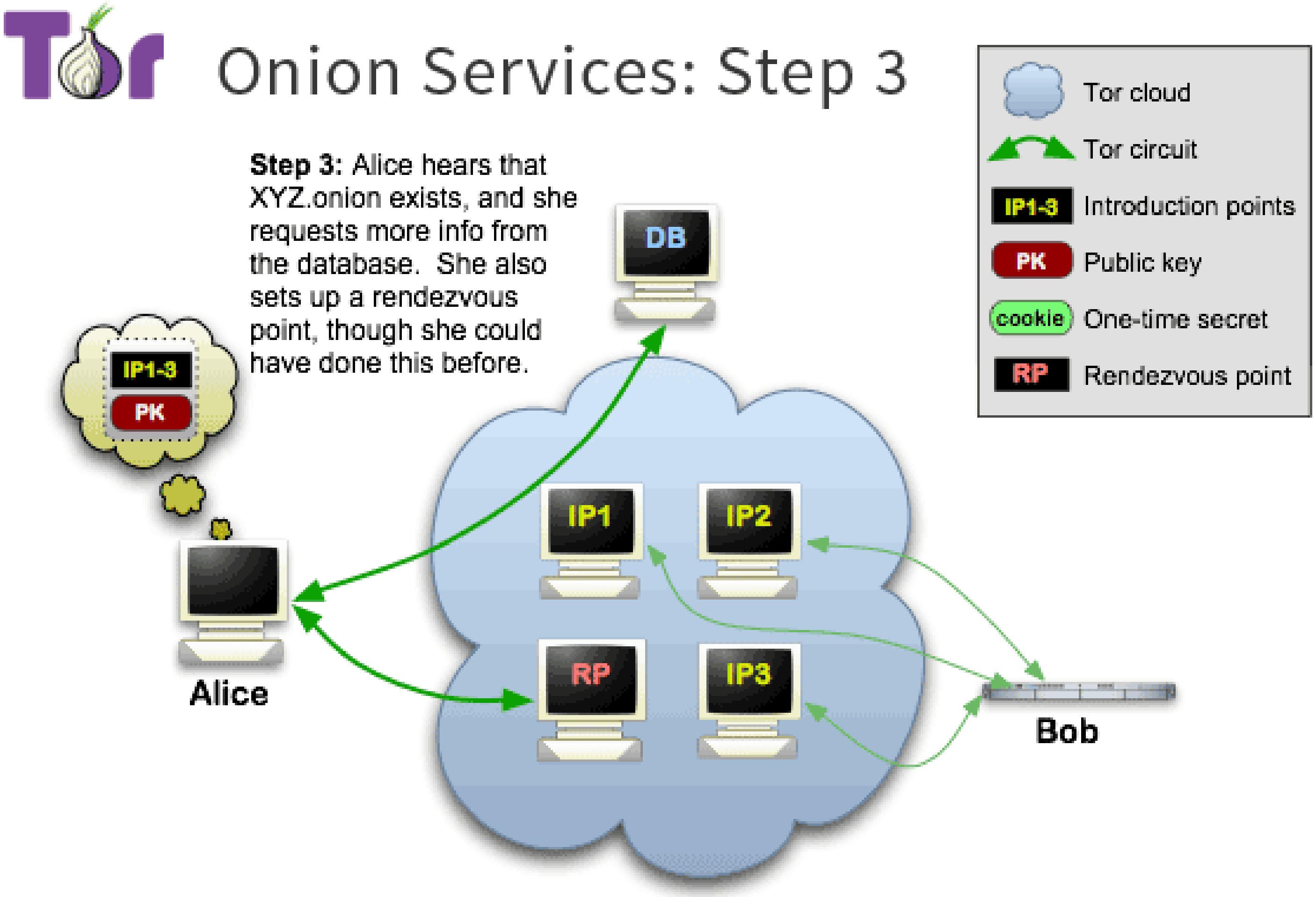
Hidden services

- **A customer who wishes to contact a hidden service must first know its address (XYZ.onion)**
  - Establishing the connection by downloading the descriptor from the distributed hash table

- **If there is a descriptor for XYZ.onion (the service can also be offline, deleted or there may be a typo in the service address), the client now knows all the points of introduction and the right public key**

- **The customer also creates a circuit to another randomly selected relay and asks him to act as a rendezvous point by giving him a one-time secret**

Hidden services



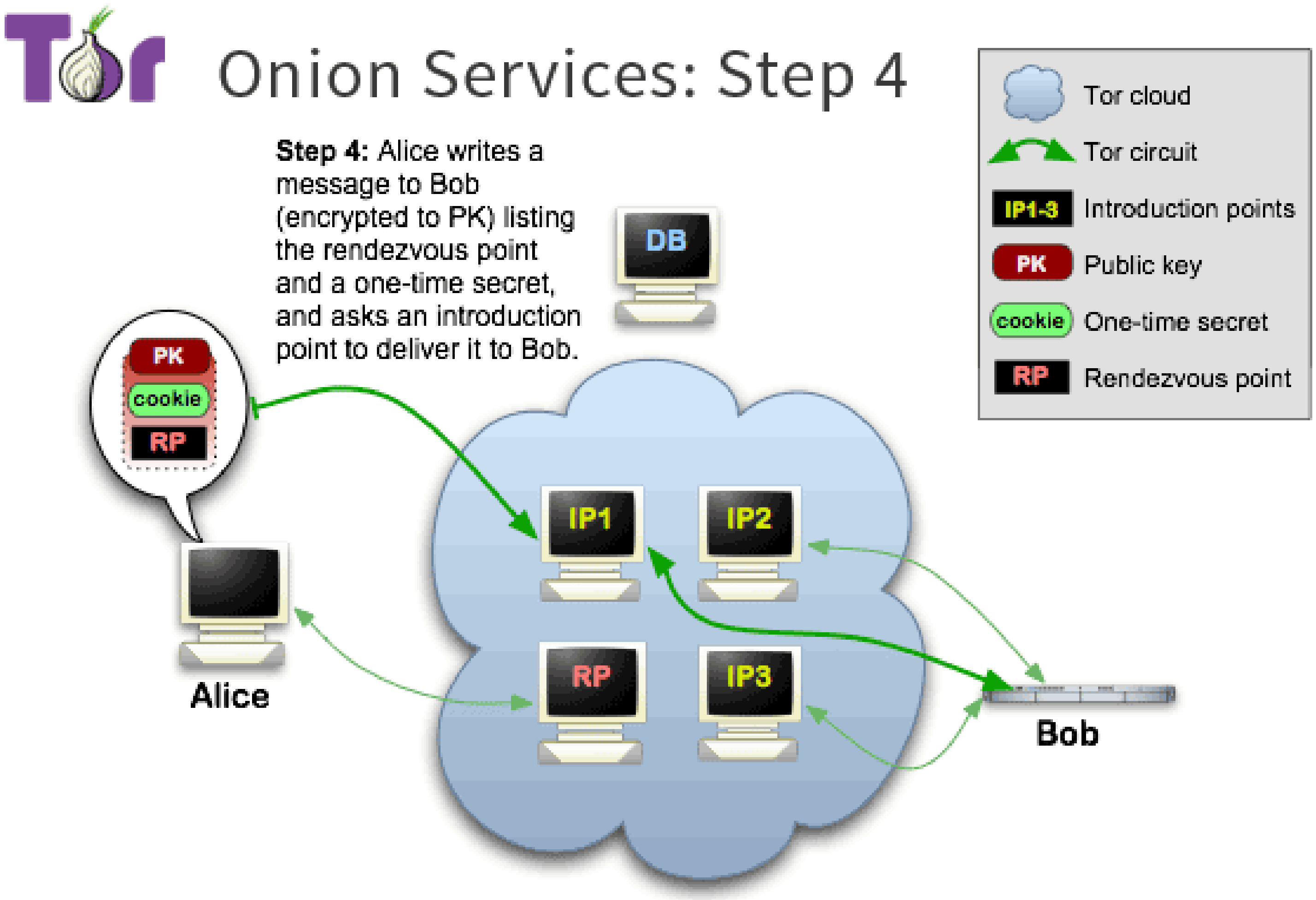
Onion Services: Step 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

Hidden services

- **If the descriptor is present and the rendezvous point is ready**
  - The customer creates an **introductory** message (encrypted with the public key of the service), including the address of the **rendezvous point** and the one-time secret
- **The customer sends this message to one of the introductory points, requesting that it be returned to the service**
- **Communication is via a Tor circuit**
  - Nobody can link the sending of the introductory message to the IP address of the client, so the customer remains anonymous

Hidden services



Onion Services: Step 4

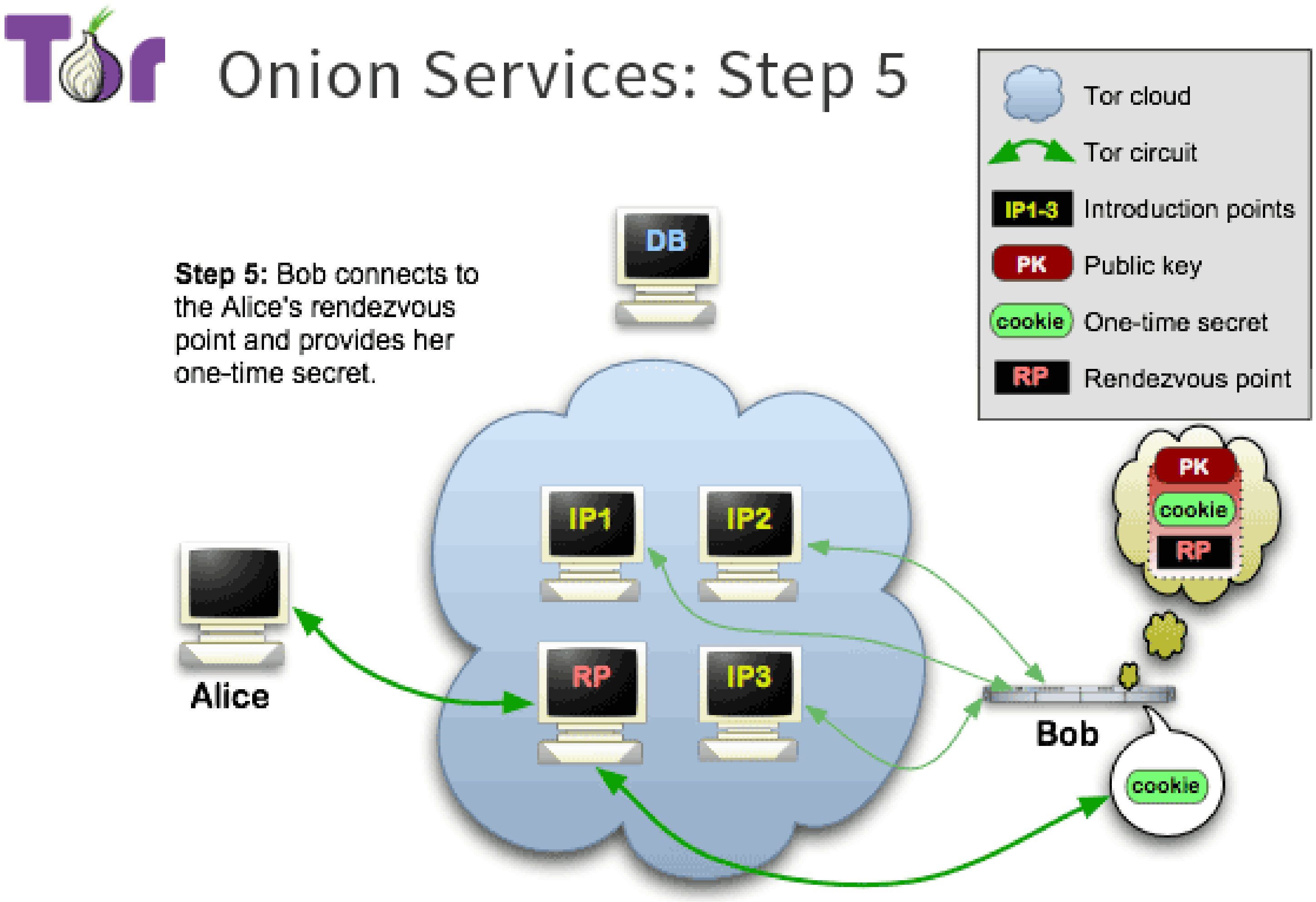
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

Hidden services

- **The hidden service decrypts the client's introductory message and finds the address of the rendezvous point and the one-time secret it contains**
  - The service creates a circuit to the rendezvous point and sends it the punctual secret in a rendezvous message

- **The hidden service must then use the same set of input circuits to avoid going through a corrupted relay to discover the IP address of the hidden service (attack Øverlier and Syverson)**

Hidden services



Onion Services: Step 5

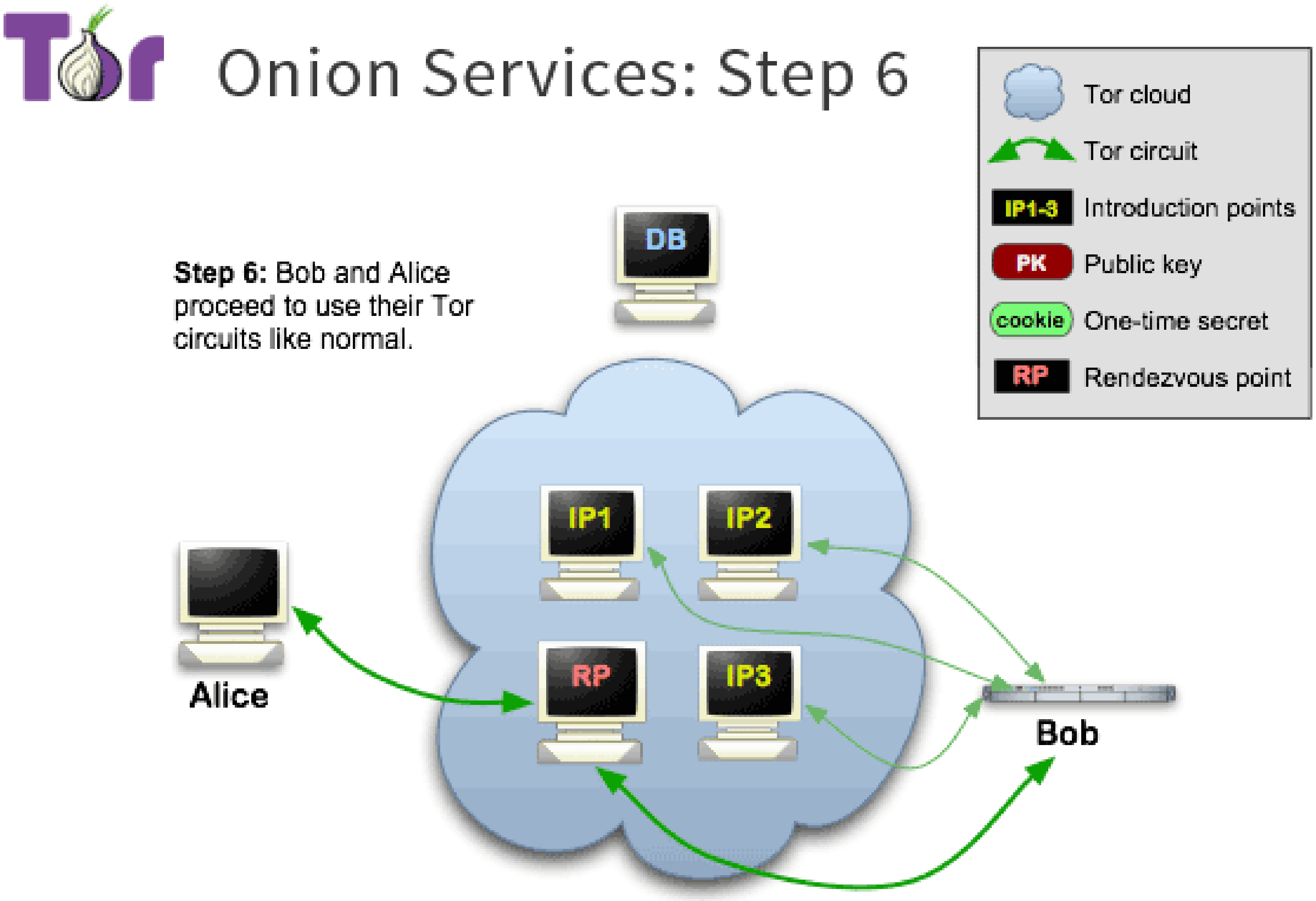
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.

Hidden services

- **The rendezvous point informs the customer of the establishment of the connection**
  - ➢ The client and the hidden service use their circuits to the rendezvous point to communicate with each other
  - ➢ The rendezvous point simply relays the messages (end-to-end encrypted) from the client to the service and vice versa

- **The complete connection between the client and the hidden service consists of 6 relays**
  - ➢ 3 of them were chosen by the client, the third being the rendezvous point and the other 3 by the onion service

Hidden services



Onion Services: Step 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.

Fall of Silk Road

Silk Road
anonymous marketplace

- **1st place in the drug market on the Dark Web**
  - Started in February 2011 and accessible only by Tor Browser
  - Worked until the arrest of its creator in October 2013
  - Its creator, Ross Ulbricht, was sentenced to life in prison
- **The investigation that led to the arrest began in the summer of 2011 with the discovery of drug trafficking by postal mail**
  - Discover the Silk Road site by querying the recipient of the package
  - The analysis of intercepted letters (type of envelope, stickers, prints) and purchase of drugs on the shops can be traced back to some dealers

Fall of Silk Road

- **This type of difficult arrest did not stop sales at Silk Road**
  - The investigators began to be interested in the administrator of the platform
  - The administrator's posts were referring to a hidden forum called “Vendor Roundtable” but only big sellers could access it
  - The same work of analysis of the letters allowed the arrest of a big salesman allowing the investigators to read the messages on the hidden forum by taking advantage of his account

- **In parallel, an FBI team manages to take the control on one of the servers of Silk Road, hosted in Iceland**
  - In the login logs of the administrator's account was the IP address of a San Francisco Internet cafe
  - In addition, the connection dates were systematically in Pacific Time format

Fall of Silk Road

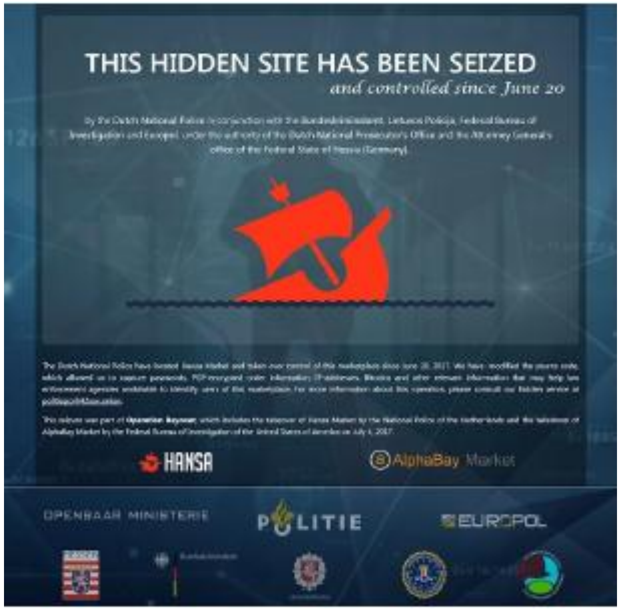
- **Retrieving an email address**
  - While searching on Google the keyword "silk road", another team of investigators found a message on Bitcointalks.org forum posted in January 2011 by a user, the first to announce the existence of a new site of sale online called Silk Road
  - The same user reveals in a message of October 2011 his personal e-mail address: rossulbricht@gmail.com. This Ross Ulbricht lives in San Francisco, near the Internet cafe whose IP address was found
  - He posted under the pseudonym "Frosty" a technical question on the forum Stack Overflow about the hidden services Tor
  - "Frosty" is also a word that appears in the Silk Road server logs and refers to the administrator's computer

Fall of Silk Road

- **Arrest**
  - Investigators discover that every time the administrator log on to Silk Road, Ross Ulbricht almost connected to Gmail at the same time
  - They engage in physical spinning and wait for the right moment to trap him in the act
  - This moment arrives in October 2013, when they see him enter a public library
  - Under the identity of the previously stopped moderator, they ask him to go to a part of the site that only the administrator can access
  - A diversion in the library allows the police to extract Ross Ulbricht's laptop on which there was an active connection under the identity of the administrator

Reduction in the use of centralized services

- **Exit-scams (platforms closing with the removal of money from customers) and the arrest and closure of Darknet sites (Silk Road, AlphaBay) are leading to a change in the habits of cybercriminals**



THIS HIDDEN SITE HAS BEEN SEIZED

and controlled since June 20

By the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hessia (Germany).

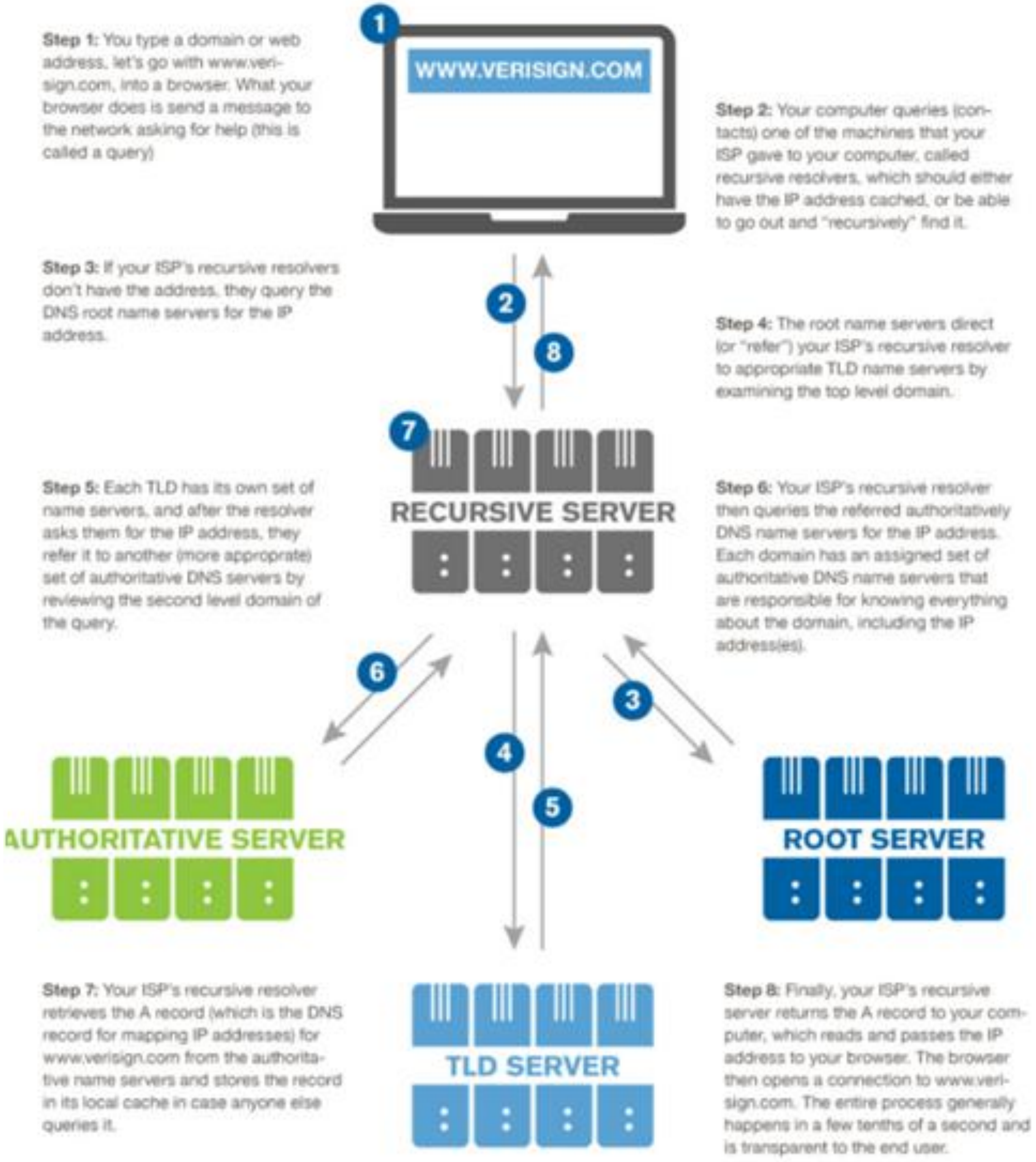
The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at [illegible].

This release was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

- **Explosion of Instant Messengers (ICQ, Jabber, QQ)**

- **Using decentralized DNS to escape censorship and blocking**
  - « Blockchain-DNS » extension on the browser
  - Blockchain domains do not have a central authority, the node network has the knowledge of all the existing sites: it is impossible for the police to make withdrawals of sites

DNS



Step 1: You type a domain or web address, let's go with www.verisign.com, into a browser. What your browser does is send a message to the network asking for help (this is called a query)

Step 2: Your computer queries (contacts) one of the machines that your ISP gave to your computer, called recursive resolvers, which should either have the IP address cached, or be able to go out and "recursively" find it.

Step 3: If your ISP's recursive resolvers don't have the address, they query the DNS root name servers for the IP address.

Step 4: The root name servers direct (or "refer") your ISP's recursive resolver to appropriate TLD name servers by examining the top level domain.

Step 5: Each TLD has its own set of name servers, and after the resolver asks them for the IP address, they refer it to another (more appropriate) set of authoritative DNS servers by reviewing the second level domain of the query.

Step 6: Your ISP's recursive resolver then queries the referred authoritatively DNS name servers for the IP address. Each domain has an assigned set of authoritative DNS name servers that are responsible for knowing everything about the domain, including the IP address(es).

Step 7: Your ISP's recursive resolver retrieves the A record (which is the DNS record for mapping IP addresses) for www.verisign.com from the authoritative name servers and stores the record in its local cache in case anyone else queries it.

Step 8: Finally, your ISP's recursive server returns the A record to your computer, which reads and passes the IP address to your browser. The browser then opens a connection to www.verisign.com. The entire process generally happens in a few tenths of a second and is transparent to the end user.

Blockchain

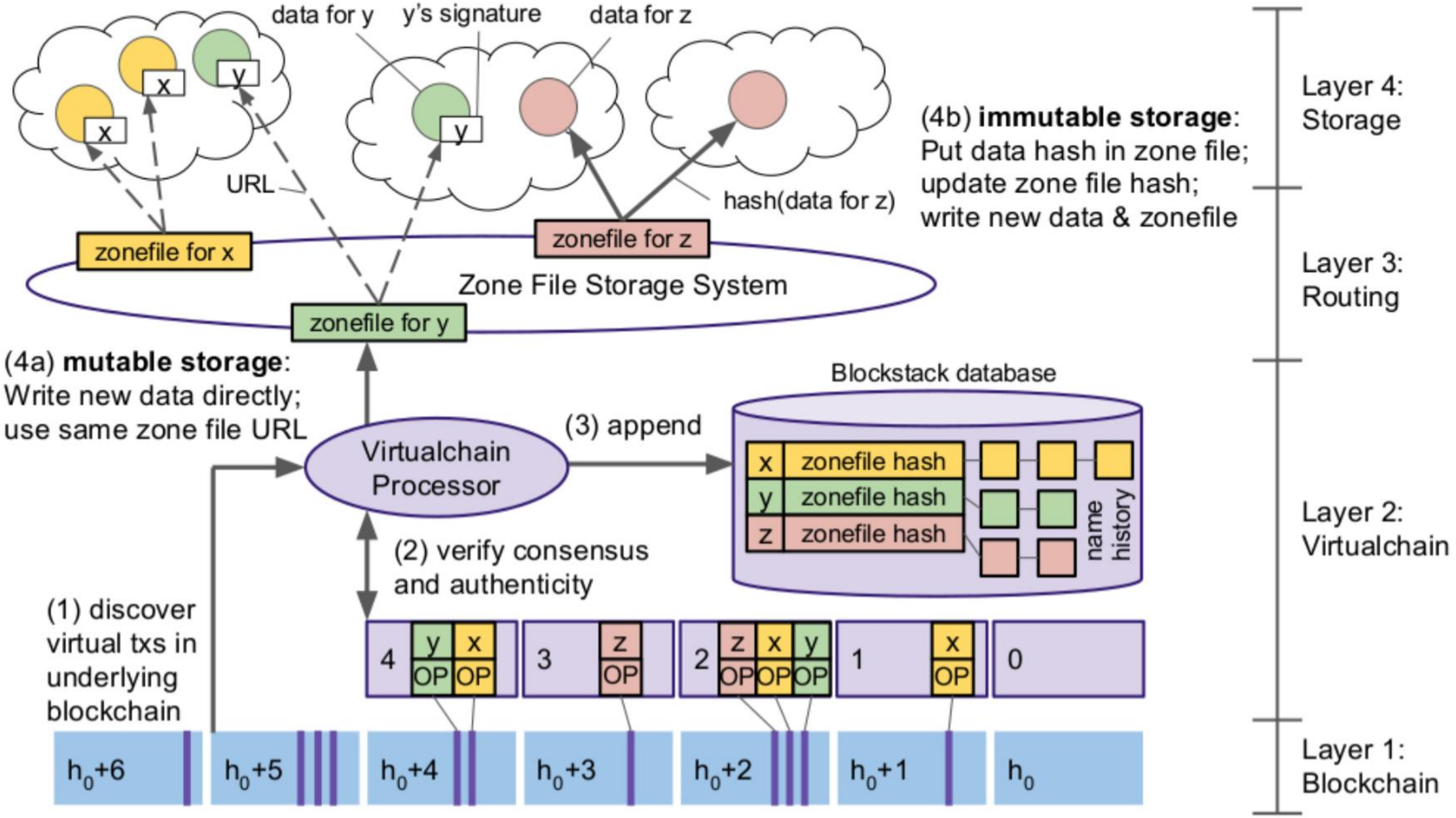
- **The blockchain is a technology of storage and transmission of information without control system**

- **Distributed database whose information sent by users and internal links to the database are checked and grouped at regular time intervals in blocks**
  - It is a **distributed and secure register** of all transactions made since the start of the distributed system

- **The 1st chain of blocks was conceptualized by Satoshi Nakamoto in 2008**
  - It was implemented the following year by Nakamoto as the main component of bitcoin, where it serves as a public registry for all transactions on the network

Blockchain-DNS

- Architecture Blockstack



Bitcoin

- **Decentralized digital currency system whose unit of account is bitcoin**
  - ➢ Bitcoin works with software and a protocol that allows participants to issue bitcoins and **manage transactions collectively** and automatically

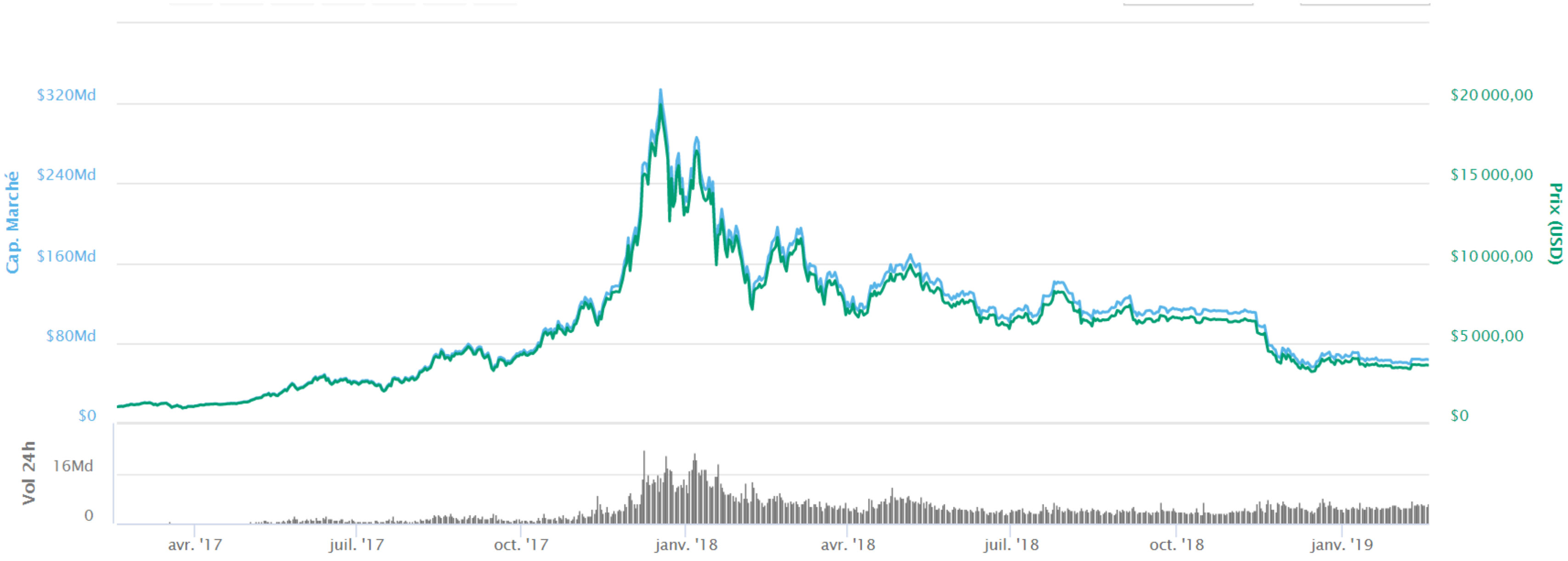
- **Bitcoin is designed to self-regulate**
  - ➢ The limited inflation of the bitcoin system is distributed homogeneously by computing power across the network, and will be limited to 21 million units divisible up to the eighth decimal

- **The smooth functioning of the exchanges is guaranteed by a totally public general organization**
  - ➢ basic protocols, cryptographic algorithms used, programs making them operational, account data

Bitcoin

The value of bitcoin is volatile

- The value of bitcoin can increase or decrease unpredictably over a short period of time due to its young economy, unexpended nature and sometimes illiquid markets



Bitcoin

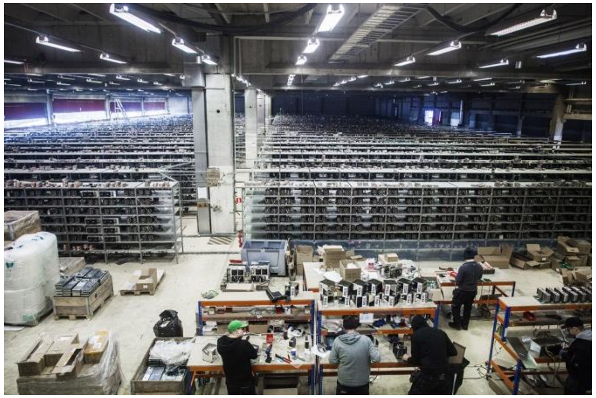
- **The possession of bitcoins is materialized by a key allowing the expense of bitcoins associated with it on the register**
  - A person may hold multiple keys in a “bitcoin wallet", a web keychain, software or hardware that provides access to the network to perform transactions
  - The keychain allows to consult the balance in bitcoins and the public keys intended to receive payments

- **To have bitcoins on an account, you have to**
  - Either go through an exchange platform that **converts** classic currencies into bitcoins
  - Either a bitcoin holder **gave** you some (sale of a good)
  - Either have **earned** them by participating in collective currency control operations

REGISTER
or
BITCOIN
EXCHANGE
BUY BITCOINS FOR USD & EUR
simple: link a payment card and fund your

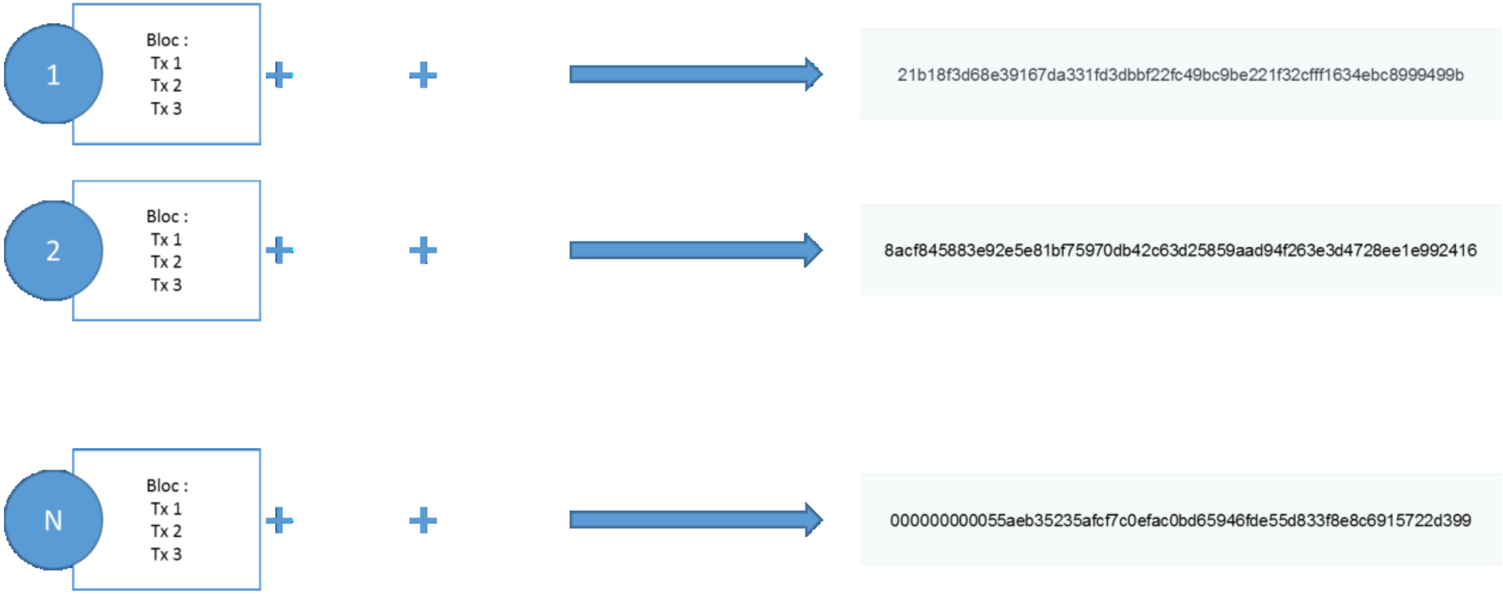
Mining

- **Miners are entities whose role is to supply the network with computing power to update the decentralized database**
  - For this update, the miners must **confirm** the new blocks by **validating the data**
  - To **add blocks** to the chain, you have to solve a **brute force** cryptography problem
  - Depending on the difficulty of the chain at the time of the resolution, they may need to **repeat several hundred billion times** the same operation
  - In the case of bitcoin, a miner is only **paid for his work provided** if he was the **first to solve** the cryptographic problem



Mining

- The proof of work consists to ask the miners to calculate the hash of the data in the block being created (containing the fingerprint / hash of the previous block), data of the miner and a random number, in order to find a hash which starts with a defined number of zeros



1

Bloc :
Tx 1
Tx 2
Tx 3

+ +

21b18f3d68e39167da331fd3dbbf22fc49bc9be221f32cfff1634ebc8999499b

2

Bloc :
Tx 1
Tx 2
Tx 3

+ +

8acf845883e92e5e81bf75970db42c63d25859aad94f263e3d4728ee1e992416

N

Bloc :
Tx 1
Tx 2
Tx 3

+ +

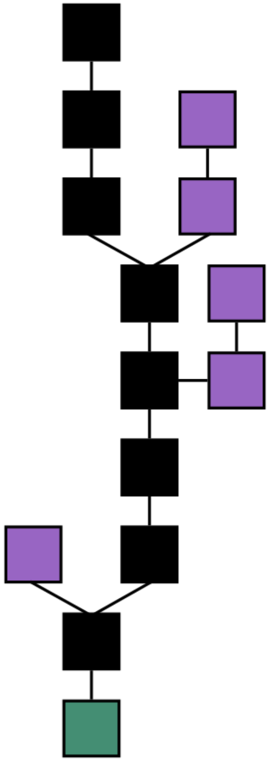
000000000055aeb35235afcf7c0efac0bd65946fde55d833f8e8c6915722d399

Mining

- **If several miners arrive at a result at a very close time, a new branch can be created**

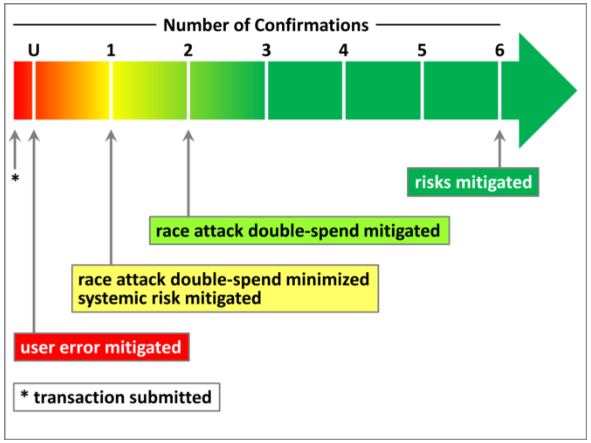
- **When there is an extra block on one branch rather than another, then the secondary branch is abandoned, and only the main branch wins**

- **To modify a transaction validated by a previous miner, it would be necessary to add a new branch that is longer than the main branch, containing the element that we want to modify**
  - ➢ It would be necessary to generate enough blocks to make the branch that is created, the main branch. However, the chance of creating blocks is proportional to the computing power of the miners → requires to possess the **majority of the computing power** available on the network (51%)



Mining

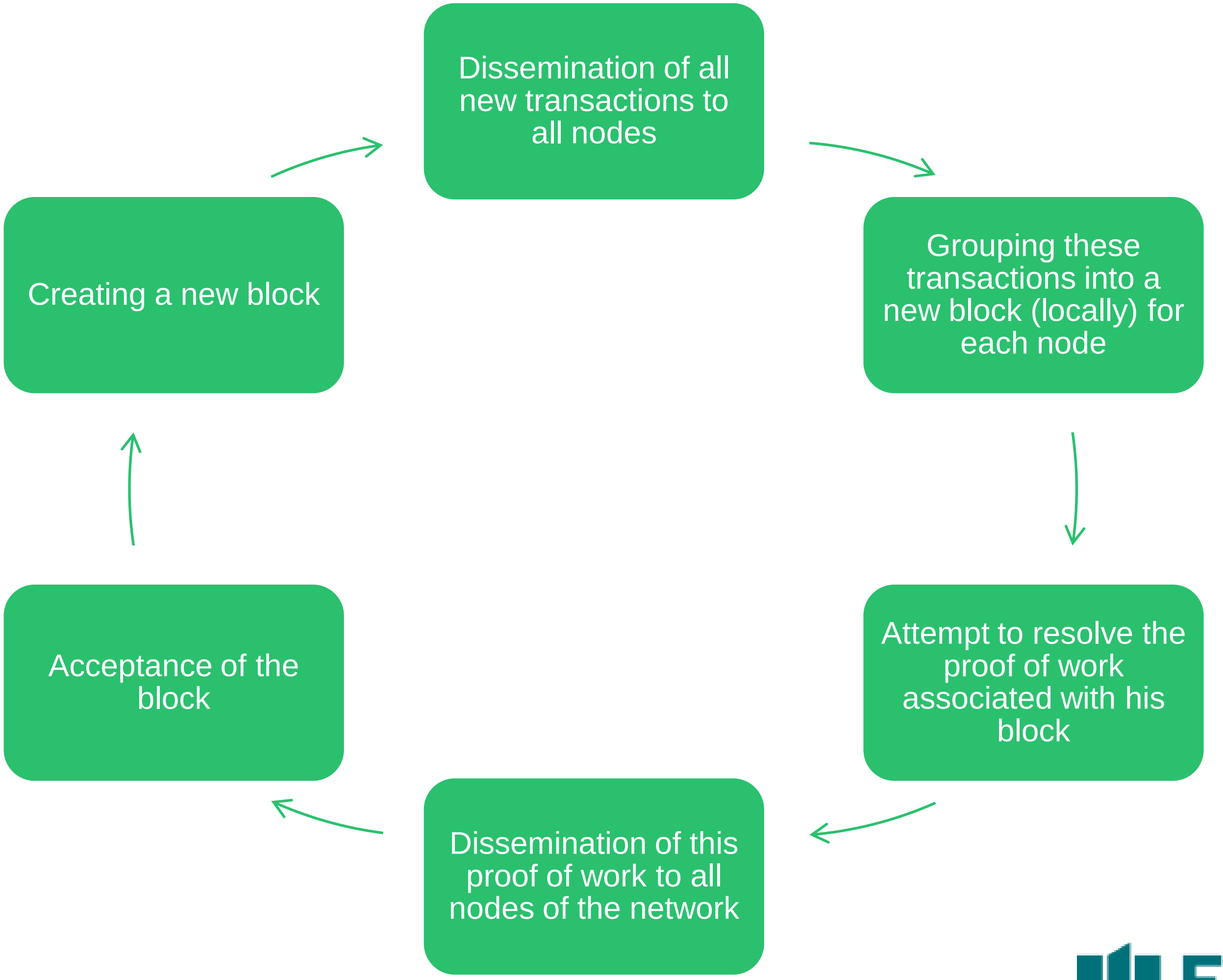
- **Mining is a distributed consensus system that is used to confirm pending transactions by including them in the blockchain**
  - One confirmation provides a good level of security
  - For large payments, wait until a transaction has accumulated more confirmations (typically 6)
  - Each new confirmation decreases the risk of a reversal exponentially



- **Mining imposes a chronological order in the blockchain, protects network neutrality and allows network computers to agree on the state of the system**
  - Every 10 minutes or so, a block is added to the blockchain via the mining

Mining

- **The nodes of the network follow the following rules**



Dissemination of all new transactions to all nodes

Grouping these transactions into a new block (locally) for each node

Attempt to resolve the proof of work associated with his block

Dissemination of this proof of work to all nodes of the network

Acceptance of the block

Creating a new block

Remuneration of miners

- **Two methods reward the energy and time-consuming calculation performed by the miner who has passed the proof of work**
  - ➢ The first transaction of the created block is a specific transaction that generates a certain amount of cryptocurrency belonging to the creator of the block
  - ➢ Transaction fees can pay miners
    - ✓ When the maximum amount of cryptocurrency is injected into the network, the **transaction fee** system will be the only economic model on which the miners will rely

- **In 2008, the reward awarded to miners was 50BTC per block mined**
  - ➢ Every 210 000 blocks mined (about 4 years), the remuneration is divided by 2
  - ➢ Today the reward is 12.5 BTC (40 000 €)