

1960



"Evolution historique de la cybersécurité depuis les années 1960"

Guillaume Jeunot

jeunot_g@hotmail.com

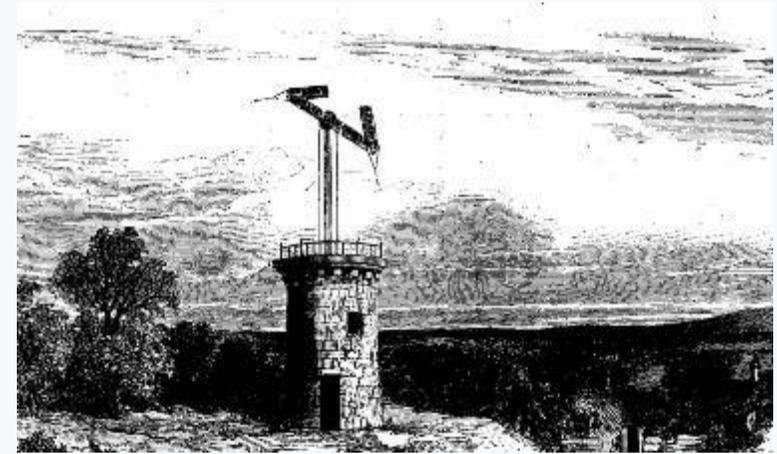
La première attaque « cyber ».

Acteurs: François et Louis Blanc, à la tête d'une société de placement à Bordeaux.

Objectif: Connaître avant les autres si les cours étaient en hausse ou en baisse à Paris.

Comment: En soudoyant un agent pour injecter dans un message officiel une « erreur » pour dire que le marché est en hausse ou en baisse.

1834



Télégraphe de Chappe



François Blanc

Programme

Le cyber, de quoi parle-t-on?

Les risques

Les aspects de la cybersécurité

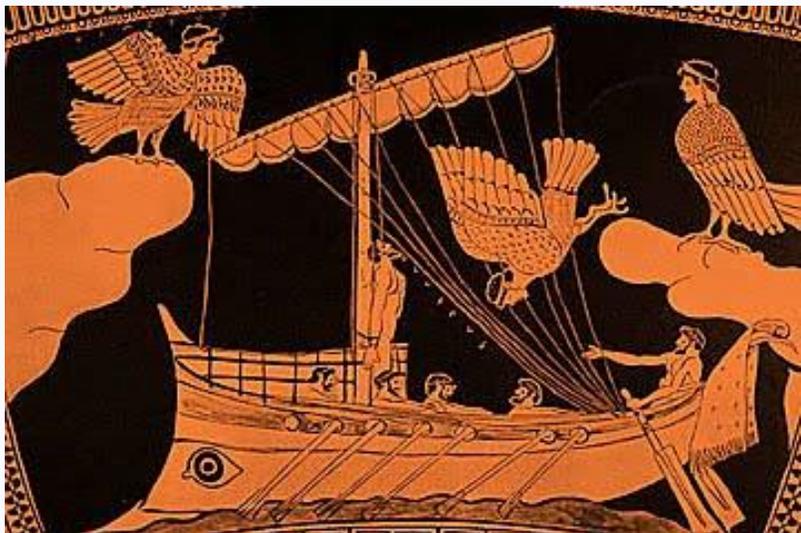
1ère partie:

Le cyber, de quoi parle-t-on?

Le préfixe « cyber »

Le préfixe cyber vient du mot grec kubernêtikê signifiant «gouvernail».

Il est usuellement utilisé comme préfixe pour former des mots relatifs à l'utilisation d'Internet, de l'informatique et de la robotique.



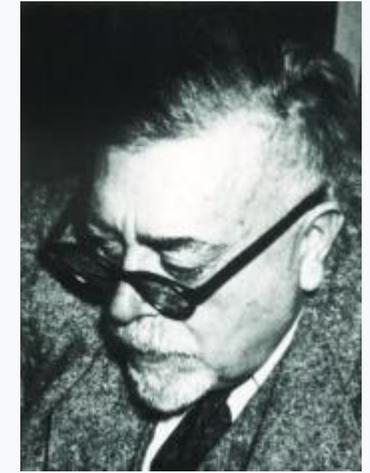
La « cybernétique »

1947

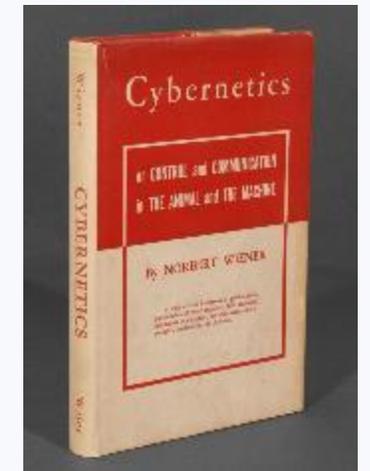
Le terme « cybernétique » apparaît sous la plume de Norbert Wiener (1894 -1964), mathématicien américain, théoricien et chercheur en mathématiques appliquées.

Le terme est développé dans son ouvrage « Cybernetics or control and communication in the animal and the machine » en 1947.

Désigne l'étude des mécanismes d'information des systèmes complexes.



Norbert Wiener



Edition 1948

Le « cyberspace »

1980

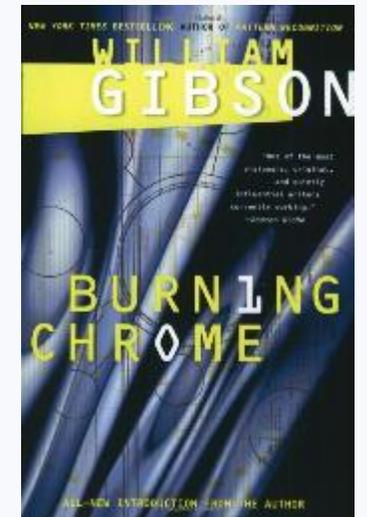
Le terme « cyberspace » apparait dans l'ouvrage de William Gibson « Burning chrome ».

Il est traduit de l'anglais cyberspace (contraction des termes Cybernetics et Space)

Désigne l'ensemble de données numériques constituant un univers d'information au sien d'un réseau mondial d'ordinateurs.



William Gibson (1948)



Burning chrome

Les origines

Au début des années 1960 né l'idée du premier réseau de communication distribué.



Mais plongeons dans l'histoire et retrouvons-nous en pleine guerre froide...



1961

Programme pour le commandement des bombardements stratégiques

19 avril 1961

Baie des cochons

Contre-attaque de forces armées cubaines



Site de lancement de missile à Cuba
en novembre 1962

Trouver une réponse à une question cruciale



Comment garantir les
moyens de
communication de
commandement
stratégique en cas de
conflit?



1^{ers} travaux d'interconnexion d'ordinateur



Au sein du Lincoln Laboratory
Joseph Licklider lance les premiers
travaux d'interconnexion
d'ordinateur.

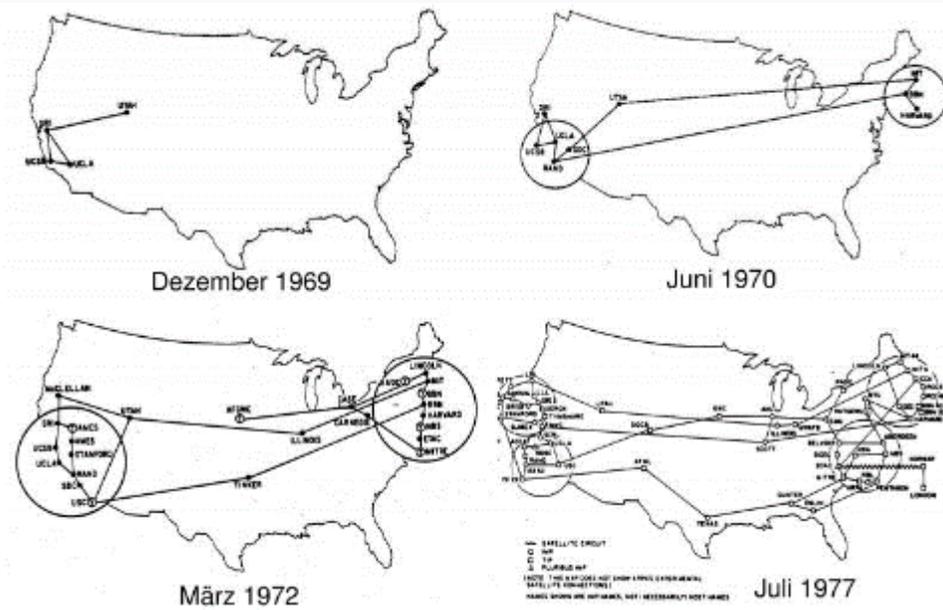
Repose sur la « transmission par paquets », technique
utilisée pour le transfert de données informatiques dans
des réseaux spécialisés.

Chaque paquet est composé d'un en-tête contenant des
informations sur son contenu et sa destination. Cela
permet à un commutateur d'aiguiller le paquet sur le
réseau vers son point final.

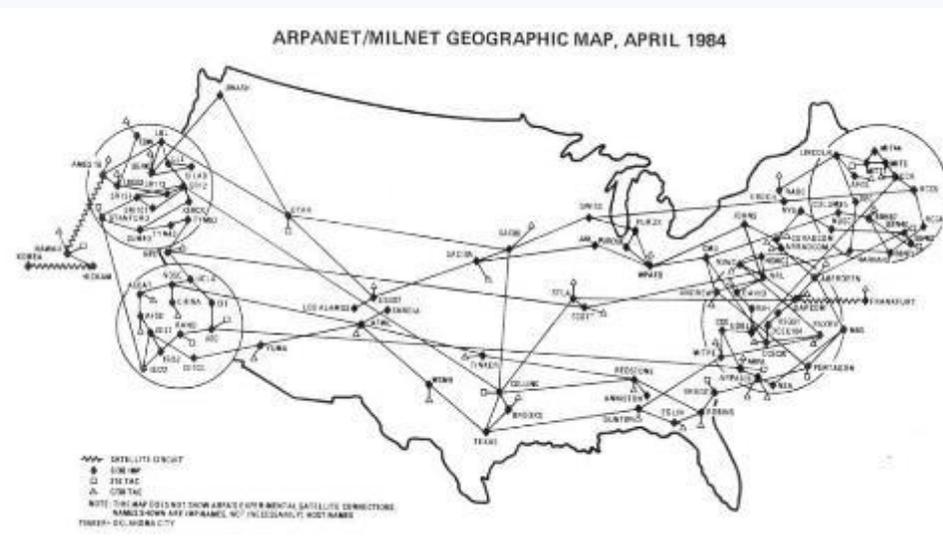


Joseph Carl
Robert Licklider
(1915-1990)

L'ARPANET



En 1969 les ordinateurs peuvent enfin communiquer entre eux malgré de longues distances.



Naissance de TCP/IP



TCP et IP sont deux protocoles de réseau informatique distincts.

IP est la partie qui obtient l'adresse à laquelle les données sont envoyées. TCP est responsable de la livraison des données une fois que cette adresse IP a été trouvée.



Nativement non pensé pour être sécurisé

Application

Services applicatifs, établit les sessions entre deux application. Encode, encrypte et compresse les données.

Transport

Etablit, maintien et termine les sessions entres les périphériques terminaux.

Réseau

Adresse les interfaces et détermine les meilleurs chemins à travers les réseaux.

Accès au réseau

Cable et connecteurs. Adresse localement les interfaces et livre les informations grâce au adresse MAC.

1960: Conception du AN/FSQ-32 par IBM pour la Strategic Air Command

1961: Defense Advanced Research Projects Agency (DARPA) conçoit un programme pour le commandement des bombardements stratégiques avec l'utilisation du AN/FSQ-32

1962: Premier travaux d'interconnexion de centres de recherches américains.

1974, le TCP/IP (Transmission Control Protocol et Internet Protocol) est créé pour uniformiser le réseau; il est toujours utilisé de nos jours.

1980, Arpanet se divise en deux réseaux distincts, l'un militaire (MLNET, de Military Network, qui deviendra le DDN — Defense Data Network) et l'autre, universitaire (NSFnet)⁵, que les militaires abandonnent au monde civil. La réflexion des constructeurs s'oriente vers une informatique décentralisée.

Le 1er janvier 1983, ARPANET adopte le TCP/IP qui sera la base d'Internet.

L'ère du Web

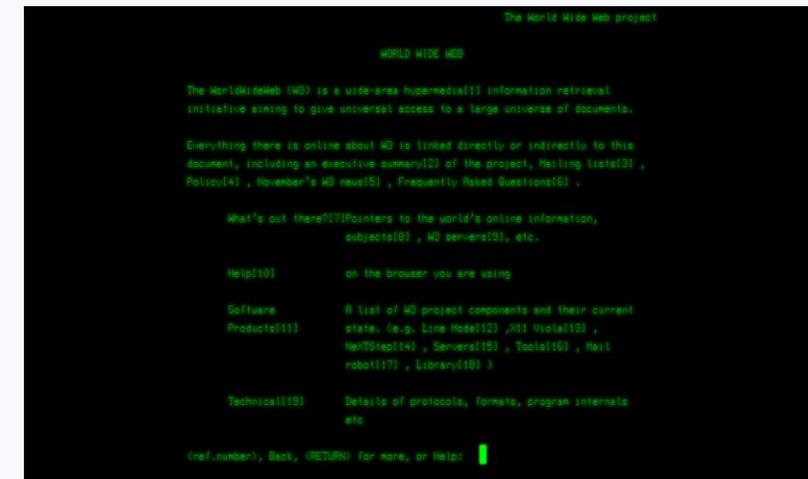
1989

Tim Berners-Lee, chercheur britannique, crée le Web au CERN.

Le projet baptisé « World Wide Web », doit permettre aux scientifiques de s'échanger des informations instantanément.



Tim Berners-Lee (1955)



Premier site Web créé au CERN

Internet, web, ...



Internet est un réseau de réseaux informatiques mondial.

Les principaux **services offert par Internet** sont le **web**, la messagerie électronique (e-mail), les forums, le chat et le FTP.

..., deepweb, darknet, darkweb, Tor

Le **deepweb** est la partie de l'internet indexable mais non-indexée.

Les **darknets** sont des réseaux superposés qui héberge une partie du deepweb, le **darkweb**.

Ces mécanismes permettent de créer de façon anonyme une ressource web (pour du contenu illégal mais pas que). Des outils tendent à préserver la confidentialité.

TOR (The Onion Router) est de loin le plus connu et le plus important de ces outils darknets.



Cyberespace c'est



Couche physique

```
Command Prompt
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

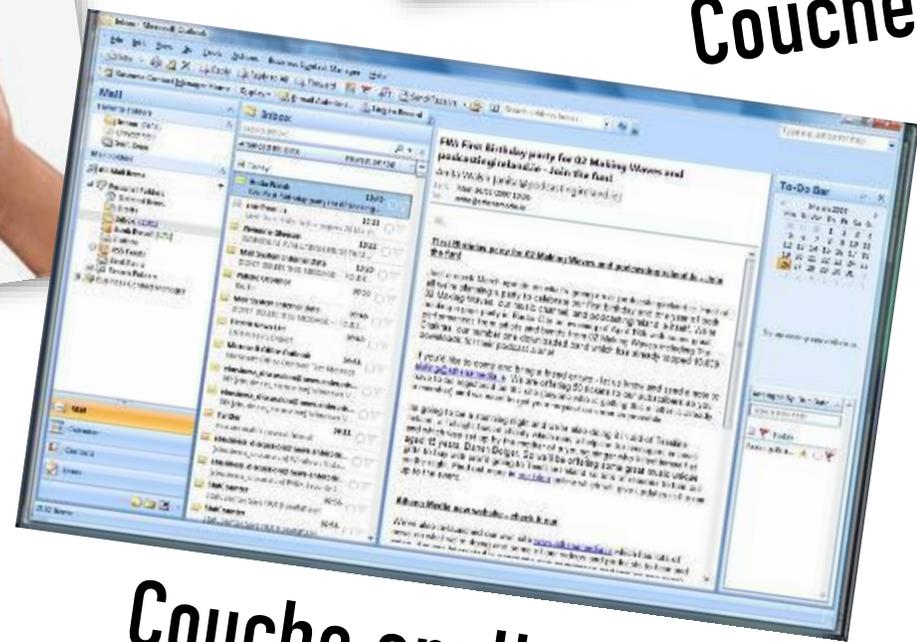
C:\Users\Michel>ping www.google.com

Pinging www.google.com [172.217.19.228] with 32 bytes of data:
Reply from 172.217.19.228: bytes=32 time=39ms TTL=53
Reply from 172.217.19.228: bytes=32 time=47ms TTL=53
Reply from 172.217.19.228: bytes=32 time=58ms TTL=53
Reply from 172.217.19.228: bytes=32 time=44ms TTL=53

Ping statistics for 172.217.19.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 39ms, Maximum = 58ms, Average = 47ms

C:\Users\Michel>
```

Couche logique



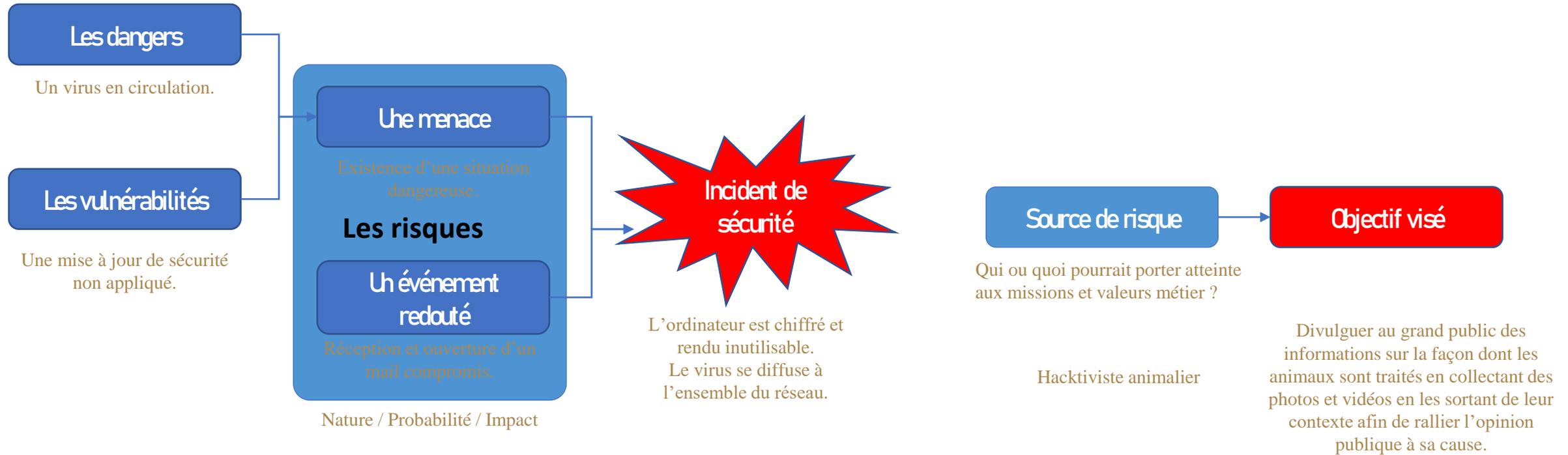
Couche applicative



Couche cognitive

2ème partie: Les risques

C'est quoi un risque



C'est la possibilité qu'un événement redouté survienne et que ses effets perturbent les missions de l'objet étudié.

<https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf>

C'est quoi un virus



En 1939 dans son article « Théorie et organisation des automates complexes », John von Neumann évoque la possibilité pour un programme de prendre le contrôle d'un autre programme.

Aujourd'hui un virus est un programme informatique malveillant qui a pour objectif de perturber le fonctionnement normal d'un appareil informatique voire de dérober des informations.

<https://www.cybermalveillance.gouv.fr/>



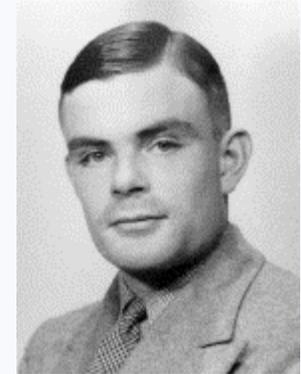
John von Neumann
(1903-1957)

Les débuts de l'informatique

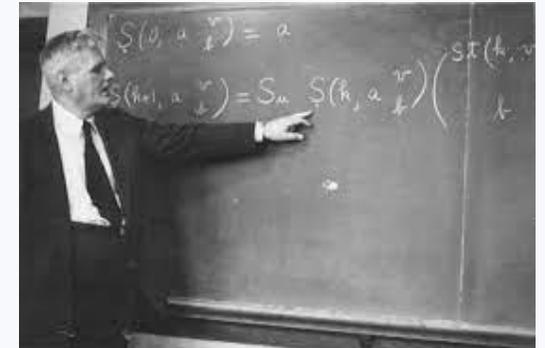
1943

En informatique théorique, une machine de Turing est un modèle abstrait du fonctionnement des appareils mécaniques de calcul.

La thèse de Church postule que tout problème de calcul fondé sur une procédure algorithmique peut être résolu par une machine de Turing.



Alan Turing
(1912-1954)



Alonzo Church
(1903-1995)

L'ENAC est le premier ordinateur reprogrammable

1945

```
nds, Memorysize, Co  
provisation_max  
ayMemory(Pitch_num,  
do  
ionrate then  
pitch ←  
armonyPitch(Harmonies, Pitch_i);  
PitchAdjustrate then  
Harmonyipitch ←  
AdjustPitch(RandomHarmonyipitch);  
else  
Harmonyipitch ← RandomHarmonyipitch;  
end  
else  
Harmonyipitch ← RandomPitch(Pitch_bounds);  
end  
end  
nd  
valuateHarmonies(Harmony);  
ost(Harmony) ≤ Cost(Worst(Harmonies)) th  
orst(Harmonies) ← Harmony;  
mony_best;
```



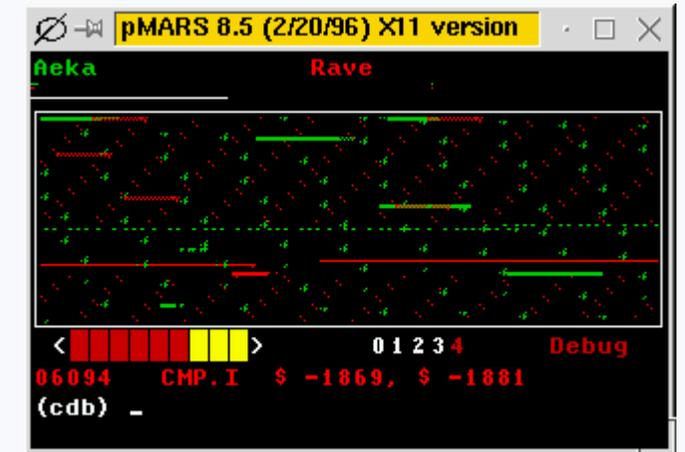
Electronic
Numerical
Integrator And
Computer est en
1945

La concurrence entre machine

Core War est un jeu de programmation dans lequel deux programmes informatiques (ou plus) sont en concurrence pour le contrôle d'une machine virtuelle.

Ces programmes sont chargés dans la mémoire vive d'une machine virtuelle et vont s'attaquer mutuellement jusqu'à ce que l'un d'entre eux plante ou ne puisse plus évoluer (ou, autre règle, si l'attaquant arrive à se reproduire dans les cellules de l'attaqué).

Ce jeu met donc en œuvre et optimise des fonctions qui seront toutes utilisées, plus tard, par les virus et les vers informatiques.



Core War 1984

1966 : dans sa Théorie des automates auto-reproducteurs, le scientifique hongrois John von Neumann théorise le premier virus.

1971: Virus Creeper, démontrer qui est possible de se déplacer sur le réseau Arpanet.

1982: Virus Elk Cloner, premier virus diffusé propagé par une disquette.

1986: « (C) Brain » développement d'un virus afin d'évaluer le nombre de copies illégales



"I'm the Creeper, catch me if you can!"

L'ingénierie sociale

Kevin Mitnick, né le 6 août 1963 à Van Nuys en Californie, est un ancien pirate informatique américain, devenu depuis les années 2000 consultant en sécurité informatique.



En 2002, il théorise l'utilisation des failles humaines pour casser la sécurité d'un système d'information dans « L'Art de la supercherie ».



Kevin Mitnick
(1963)

Par exemple, pour attaquer des éditeurs de logiciel on va cibler des sites d'astuces que consultent habituellement des développeurs.

En 2012, une attaque de point d'eau permet d'infecter plus de 500 entreprises en 24 heures

L'ingénierie sociale – les traces



Menu

e Police, 19 Av. de Paris, 78000 Vers

l'Ermitage, 78000 Versaill APPARTEMENT

Ajouter une destination

Partir maintenant Options

Envoyer l'itinéraire vers votre téléphone

via Av. de Paris 9 min
Le plus rapide, malgré un trafic aussi dense que d'habitude 2,4 km

Détails

e de l'Ermitage, 7
Estimations de prix MeilleursAgents au 1 fé

Prix m2 moyen
9 733 €
de 7 522 € à 11 852 €
Indice de confiance ●●●●● M

Thomas
Juniste Confon.
Versailles, Île de France, France · 139 relations

Inscrivez-vous pour entrer en relation

Activité

LA SÉCURITÉ DES DONNÉES PERSONNELLES

RGPD | La sécurité essentielle de

Thomas I

- C'est ça fessier, c'est
- VERSAILLES

Ajouter

Profil

COPAINS

- François G. VERSAILLES
- Athilde
- File MC. VERSAILLES

TotalEnergies
World of Energy

Wires offres d'emploi

L'ingénierie sociale – les faux profils

14b/

Recherche

Accueil Réseau Emplois Messagerie

Nicole Garnier · 2e

Chargée de recrutement MAAF/Groupe COVEA - Alternante en Master RH chez MAAF Assurances - Groupe Covéa
Niort, Nouvelle-Aquitaine, France · + de 500 relations · [Coordonnées](#)

[Se connecter](#) [Message](#) [Plus...](#)

AXA Investment Managers
 IUT Techniques de Commercialisation (La...)

L'essentiel

18 relations en commun
Nicole et vous connaissez Michaud Stéphane, Arnaud RIVIERE, et 16 autres personnes

Activité

1369 abonnés

Les posts que Nicole a créés, partagés ou commentés au cours des 90 derniers jours sont affichés ici.

[Voir toute l'activité](#)

Expérience

Conseillère client Axa
AXA Investment Managers
sept. 2018 – Aujourd'hui · 2 ans 7 mois

AXA est un groupe international français spécialisé dans l'assurance depuis sa création, et dans la gestion d'actifs depuis 1994.

Nadine Wilson Njeim



Cet article est une **ébauche** concernant un **mannequin libanais**.

Vous pouvez partager vos connaissances en l'améliorant (comment ?) selon les recommandations des projets correspondants.

Nadine Wilson Njeim, en arabe : نادين ويلسون نجيم, née le 8 février 1988 à *Maaser El Shouf* au Liban, est la *Miss Liban 2007*¹. Elle représente son pays à *Miss Monde 2007* en Chine et *Miss Univers 2007* à Mexico. Depuis elle mène une carrière d'actrice à la télévision et est la voix arabe de Lara Croft, dans le jeu vidéo *Tomb Raider* de 2013².

Elle a étudié le commerce international et s'est spécialisée en affaires internationales à l'Université Américaine de Beyrouth.

Le 27 août 2016, elle épouse l'amour de sa vie Ramzy DIB

Nadine Wilson Njeim

نادين ويلسون نجيم



Nadine Wilson Njeim en 2007.

mdr
marque de repères

Le podcast qui scrute les
sujets d'actualité et digite.

[Rechercher un podcast](#)

Des idées d'informations.

JERES NOUVELLES

Un podcast mettant en
lumière les histoires de
femmes du globe
Persique

BIJOUX

Modèles de bagues en
or blanc et les modes
contemporaines. Les plus

n_564833456_161904017555166_135616

Les biais cognitifs

Ou la faille entre la chaise et le clavier

En 2016, lors des élections américaines, les Russes créent des identités fictives sur les réseaux sociaux pour influencer les opinions des citoyens américains.

En 2020, TripAdvisor annonce détecter près d'un million de faux avis soumis à sa plateforme (soit 3,6 % du total des messages).

Exemples de biais:

- le biais de confirmation consiste à ne porter attention qu'aux éléments allant dans le sens de son point de vue initial;
- le biais de conformité conduit à prendre des décisions similaires à celles de pairs, alors que la situation n'est pourtant pas la même;
- le biais d'informations désigne la tendance à chercher toujours plus d'informations, même inutiles, en pensant que cela générera une meilleure décision.

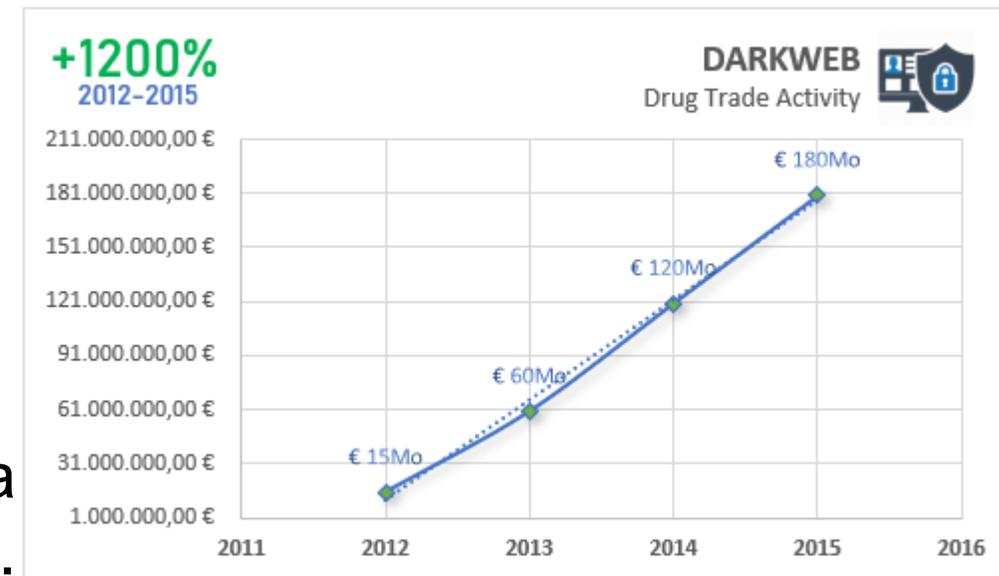


Une véritable industrie de la cybercriminalité

RANSOMWARE	PRICE (USD)
Custom Stealer Ransomware BTC	\$199
Code Source Bitcoin Thief & Ransomware BTC	\$99
Intelligent Bitcoin Thief Copy/Paste Source Code/Ransomware Modified 2017 More Agressive	\$50
Android Locker Ransomware	\$250
Ransomware - Custom Made	\$1470
Ransomware Pigsaw Source Code Modified 2017	\$30
Personal Custom Stealer & Ransomware BTC	\$75
Source Code Bitcoin Thief & Ransomware BTC HQ	\$50
Intelligent Bitcoin Thief Copy/Paste Source Code/Ransomware Modified 2017 More Agressive	\$25
?Code Source Bitcoin Thief & Ransomware BTC???	\$99
6 Bitcoin Ransomware Easy Money System	\$5
Philadelphia Ransomware and Other Make Top \$\$\$ (Clone)	\$1
Custom Stealer & Ransomware	\$50

L'Unité Black chiffre qu'entre 2016 et 2017 la vente de ransomwares a augmenté de 2502 % sur le Darkweb.

En 2015 le blanchiment de l'argent de la drogue sur le darknet dépassait les 180 M €.



3ème partie: La cybersécurité

Le début de la cybersécurité

404
av JC

404 av JC, **la scytale**, ou bâton de Plutarque, était un bâton de bois utilisé pour lire ou écrire une dépêche chiffrée.

Elle est le plus ancien dispositif de cryptographie militaire connu.



Scytale

Système automatisé pour les fichiers administratifs et le répertoire des individus



Adophe Touffait, procureur général de la Cour de cassation, en avril 1973, devant l'Académie des sciences morales et politiques, s'exprimait:

« La dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques ».



La protection des données personnelles

1978



- La loi dite « Informatique et Libertés » entre en vigueur le 6 janvier 1978
- Création de la Commission Nationale de l'Informatique et des Libertés (CNIL).

1995



- Directive européenne 95/46/CE sur la protection des données personnelles.

2018



- 25 mai 2018 mise en application du règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

La Convention de Budapest



La Convention sur la cybercriminalité, dite Convention de Budapest, est le premier traité international qui tente d'aborder les crimes informatiques et les crimes dans le cyberspace.

Elle aborde les questions de la pornographie infantile, de l'atteinte au droit d'auteur et des discours de haine.

Elle harmonise certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations.

La Loi pour la confiance dans l'économie numérique 2004



- Renforcer la confiance dans le commerce électronique et la lutte contre les publicités indésirables.
- Conforter la liberté de la communication publique en ligne en France.
- Mieux sécuriser les échanges et amplifier les moyens de lutte contre la cybercriminalité.

22 juin 2004

JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE

Texte 2 sur 108

LOIS

LOI n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1)

NOR : ECCX0200175L

L'Assemblée nationale et le Sénat ont adopté,

Vu la décision du Conseil constitutionnel n° 2004-496 DC du 10 juin 2004 ;

Le Président de la République promulgue la loi dont la teneur suit :

TITRE I^{er}

DE LA LIBERTÉ DE COMMUNICATION EN LIGNE

CHAPITRE I^{er}

La communication au public en ligne

Directive Network and Information System Security

Elle vise à assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union Européenne.



4 enjeux majeurs:

- La gouvernance;
- La coopération;
- La sécurité des opérateurs de Services Essentiels;
- La sécurité des fournisseurs de services numériques.

Cybersecurity Act



Le Cybersecurity Act établit un cadre législatif et des standards uniques de cybersécurité pour l'espace européen.

Ses objectifs:

- Sécuriser les produits, services et processus;
- Construire des processus de sécurité robustes;
- Protéger les données;
- Vérifier l'absence de vulnérabilités connues;
- Garantir l'accessibilité aux accès restreints;
- Établir un historique de la donnée;
- Assurer une cyber résilience.

Mandat renforcé pour ENISA, l'European Union Agency for Cybersecurity.

Direction technique du chiffre



En 1943, le Conseil de défense de la France libre crée à Alger la “Direction technique du chiffre”. Elle a pour mission de protéger les informations échangées mais aussi contribuer, aux côtés des Britanniques et des Polonais, à casser d’autres codes.

Agence nationale de la sécurité des systèmes d'information

« L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées.

Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. »



Le Commandement de la cyberdéfense (COMCYBER)



Il est responsable de la cyberdéfense militaire. Il recouvre l'ensemble des actions défensives et offensives conduites dans le cyberspace.

Ses missions:

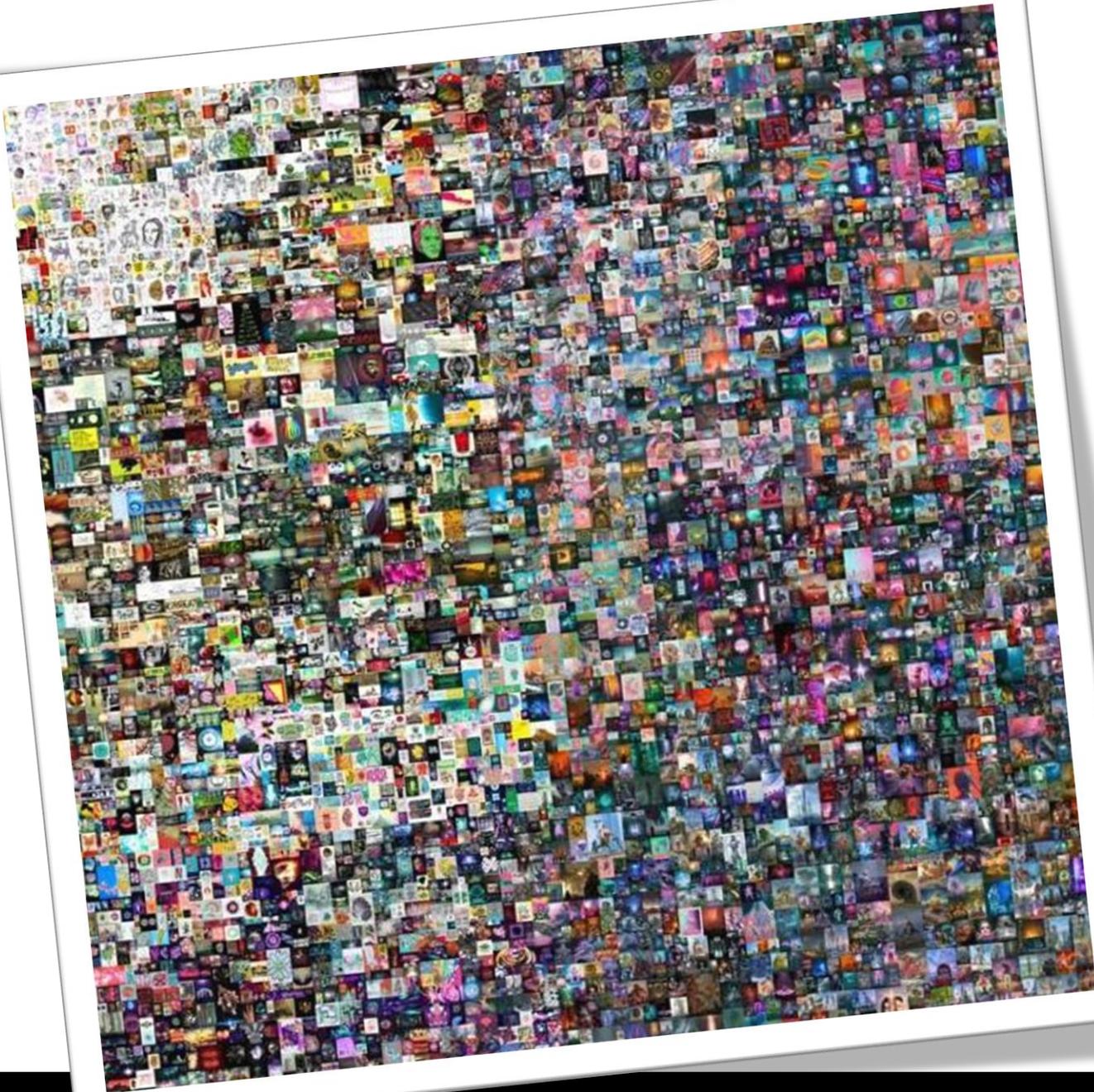
- Conçoit et planifie les opérations de cyberdéfense;
- Coordonne la stratégie;
- Contribue à la réponse capacitaire.



« Everyday : the first 5000 days »

Un fichier image JPG à

69 millions de dollars



Métavers

« Méta » vient du grec et signifie « au-delà ». Un métavers, c'est donc un univers au-delà du monde physique, un monde virtuel.

1964

Métavers, ou web 3D, est un concept décrit une première fois par Daniel Francis dans son roman Simulacron 3.

2022

Meta investit 10 milliards de dollars dans son metavers.



Daniel Francis
Galouye
(1920 - 1976)

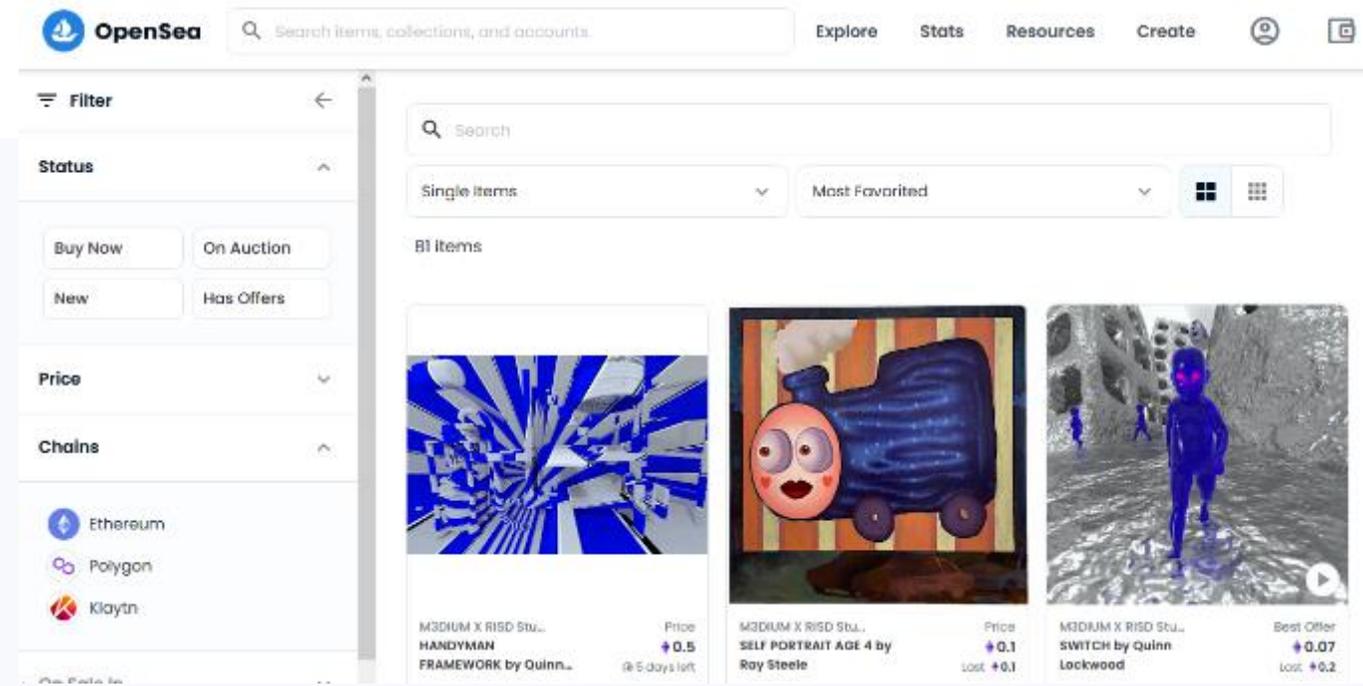


NTF ou Jeton Non Fongible



Un jeton non fongible est un jeton unique ne pouvant pas être remplacé par un autre.

Cette donnée est stockée et authentifiée grâce à un protocole de chaîne de blocs (blockchain).



OpenSea est une place de marché pour les NFT.

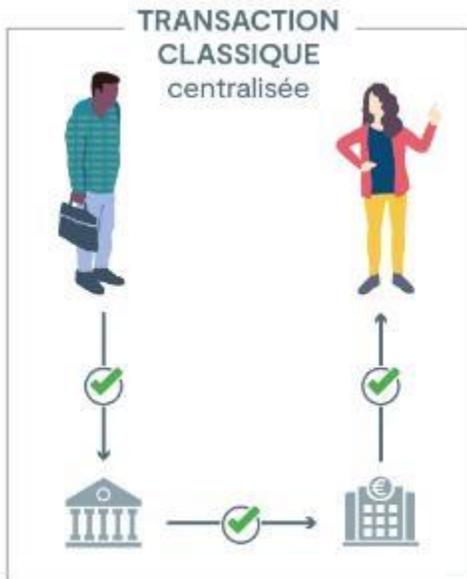
Blockchain

2008

Satoshi Nakamoto a publié un livre décrivant la monnaie numérique Bitcoin.

Une blockchain peut être assimilée à un grand livre public de transaction, anonyme et infalsifiable.

Un jeton ou cryptomonnaie correspond à la rémunération du travail de « minage », c'est-à-dire de création des blocs de transaction.



Cette base de données sécurisée et décentralisée est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

A vos questions