PV de la 26e Assemblée Générale

Porrentruy, Lycée cantonal, 27 avril 2024, 14h.

Excusé-e-s : Charles Félix, Journal Le Franc-Montagnard, Nadia et Marco Roth, Christian Vaquin

Ordre du jour

1. Bienvenue et salutations
2. Ordre du jour
3. PV 2023
4. Comptes 2023
5. Admissions, démissions, élections
7. Divers.

1. Bienvenue et salutations

Le président, Benjamin Bergé, accueille les participants à notre assemblée générale de ce jour. Il s'agit de la 26ème assemblée de notre cercle.

2. PV 2023

Le PV de la 25ème assemblée a été envoyé avec la convocation. Il est accepté à l'unanimité.

3. Comptes 2023

La trésorière, Marie-Thérèse Kohler, présente les comptes : en 2023 le CMP n'a pas reçu de subvention de la SJE. Le 31.12.2022 la fortune s'élevait à fr. 4'243.05 et le 31.12.2023 à fr. 3623.05 soit une perte de fr. 620.-.
Les comptes 2023 ainsi que le rapport des vérificateurs sont acceptés à l'unanimité.

4. Admissions, démissions, élections

Néant

5. Divers

Le président donne quelques informations liées au dernier Conseil de la SJE.

La parole n'étant plus demandée, l'AG s'achève officiellement.

Problèmes du CMP

Pierre-Olivier Vallat donne les solutions du / des problèmes 2023 et présente la mouture 2024.

Pas de prix du CMP

Aucun travail de maturité en mathématique ou physique n'était particulièrement significatif cette année pour que le prix du CMP soit attribué.

Conférence : les cryptomonnaies

Monsieur Emmanuel Benoist de Haute école spécialisée bernoise-BFH nous présente sa conférence consacrée au bitcoin et aux cryptomonnaies.

Il brosse tout d'abord un aperçu de l'histoire de la monnaie, aperçu dans lequel il relève qu'une monnaie doit être thésaurisable et avoir une valeur pour les deux parties. La monnaie traditionnelle (métal ou papier) doit être gérée par une banque centrale digne de confiance, telle que la Banque Nationale suisse, contrôlée par l'état. Avec Internet est arrivé le paiement électronique qui s'étend au-delà des frontières des états. Il s'agit donc de sécuriser ces transactions. Actuellement, la sécurité s'appuie sur des fonctions de hashage soit des fonctions simples à calculer dans un sens par exemple $z=h(x)$, mais pratiquement impossible à calculer en « marche arrière » $x=h^{-1}(z)$. SHA256 ou SHA512 sont utilisées actuellement. Pour crypter les données, on utilise une clé publique, connue de tous. Pour décrypter les données, il faut une clé privée connue par le seul propriétaire.

Le bitcoin a été inventé par Satoshi Nakamoto. Cette monnaie virtuelle est basée sur un logiciel open source. Toutes les transactions depuis l'apparition des bitcoins sont publiées dans une blockchain. La taille du fichier est actuellement de 570Gb. Elles peuvent être téléchargées sur https://blockchain.info. Elles sont validées par des volontaires qui calculent la nouvelle blockchain. Ils sont récompensés de leur travail par l'octroi de bitcoins, sortes de « pépites d'or ». Ils sont d'ailleurs appelés les « mineurs ». L'argent virtuel est stocké dans des « adresses » et une transaction fait passer de l'argent d'une adresse à une autre. Toutes les transactions sont stockées dans une gigantesque blockchain qui contient toutes les transactions depuis la naissance des bitcoins. Chaque utilisateur génère une clef publique et privée. Néanmoins, la clé publique ne sera pas utilisée telle quelle, car c'est sa valeur de hashage qui sera publiée comme adresse. Afin de garantir que l'argent n'est utilisé qu'une seule fois, tout l'argent d'une adresse doit être dépensé en une fois. Si la somme à payer est inférieure à la somme attribuée à l'adresse, la différence est attribuée à une nouvelle adresse et l'adresse qui vient d'être utilisée est définitivement désactivée. Pour des paiements plus importants, il est possible de regrouper plusieurs adresses. Toutes les transactions sont publiques puisqu'il n'y a pas de banque pour valider les transactions. C'est la communauté qui s'en charge.

Du point de vue écologique, les bitcoins sont énergivores, car tous les mineurs doivent calculer en boucle des valeurs de hachage.

Monsieur Benoist nous présente un nouveau projet de monnaie électronique, le « GNU-Taler » qui fait intervenir une banque. L'originalité du système consiste en l'anonymisation totale du paiement. L'un des plus gros avantages est la diminution drastique de l'énergie consommée. Autre avantage, la banque connaît exactement les sommes reçues par le marchand, ce qui empêche le blanchiment d'argent. Enfin, personne ne peut savoir comment le client dépense son argent. Monsieur Benoist travaille activement sur ce projet dans le cadre d'une recherche financée par l'Union européenne et la Confédération.