« BLOCKCHAIN ET PARTAGE DE L'ÉNERGIE »

David Vangulick, doctorant Université de Liège

AGENDA

- Introduction
- Definitions
- Concepts
- Création d'un bloc
- Rôle du mineur
- Choix d'une blockchain
- Le secteur de l'énergie
- Preuve d'enjeu
- Preuve de travail
- Proposition d'une chaîne synchronisée
- Conclusion

INTRODUCTION

Parler de blockchain …

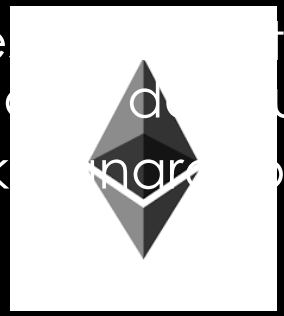
C’est ouvrir une porte vers l’inconnu

C’est faire un pas dans un monde étrange

C’est humblement admettre que tout savoir est impossible

DÉFINITIONS

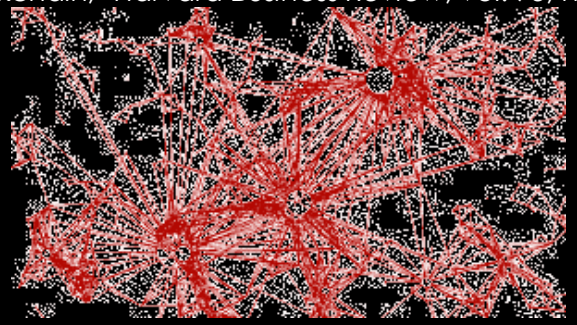
- Le blockchain n'est pas:
  - Le Bitcoin, l'Ethereum, le litcoin …
  - Réservé au dark (deep) web
  - Le moyen trouvé par de[illegible]tions mafieuses voire terroristes désireuses de passé en dessous des ra[illegible]d[illegible]utorités
  - Un truc de "crypto-punk[illegible]naro[illegible]-Trotkiste"



DÉFINITIONS

- Blockchain est
  - Un registre ouvert et distribué qui permet d'enregistrer efficacement, de manière vérifiable et permanente les transactions entre deux parties.

    (*) M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.



  - Un ensemble de technologies de cryptographie et de l'information mises ensemble pour créer un système robuste basé sur les theories du jeu et le consensus.

CONCEPTS

- Faire un échange = créer une transaction
- Prenons un exemple: le roi Edouard VII aimerait donner une maison à George (futur roi) et à sa future épouse Victoria Mary (future Queen Mary)

King
Edward VII

York Cottage

Transaction

Victoria
Mary

Georges

CONCEPTS

- Pour créer une transaction **valide,**
  - Vous devez d'abord prouver la propriété de ce que vous voulez échanger
    - Parce que vous l'avez reçu de quelqu'un (et que nous pouvons revenir à l'origine)

York Cottage

Construit en 1771, acheté par la reine Victoria et donné à Édouard VII

    - Parce que vous avez le droit de le créer (après tout, il est roi)

  - Vous devez connaître le destinataire
  - L'expéditeur doit signer

CONCEPTS

- Une manière «classique» de faire une transaction:

un fonctionnaire qui a l'autorité (légale) de dire que les transactions sont correctement signées, vraies et de faire un serment (= promesse) officiel
=> "L'homme au milieu" l'intermédiaire enregistre ces transactions dans un livre / un grand registre
Notaire - Banque - société de lecture de compteurs ...

CONCEPTS

- Ces pratiques «classiques» ont beaucoup d'inconvénients:
  - Confiance «l'homme au milieu»
    - Le processus est aussi bon que son point le plus faible: humain
    - Par exemple. Crise bancaire 2008 => le tout début de Bitcoin
  - Risque d'altération / de triche des enregistrements
  - Risque de manipulation / destruction du registre
- Pour éviter ces inconvénients: «Un banc de poisson est moins vulnérable qu'un poisson seul»

DÉCENTRALISATION

CONCEPTS

- Et si ces transactions sont gérées de manière décentralisées:

  CONSENSUS que les transactions sont **correctement signées, vraies et de faire un serment (= promesse) officiel**, **d'une manière numérique**

- Comment s'assurer que les transactions sont correctement signées et vraies d'une manière numérique:

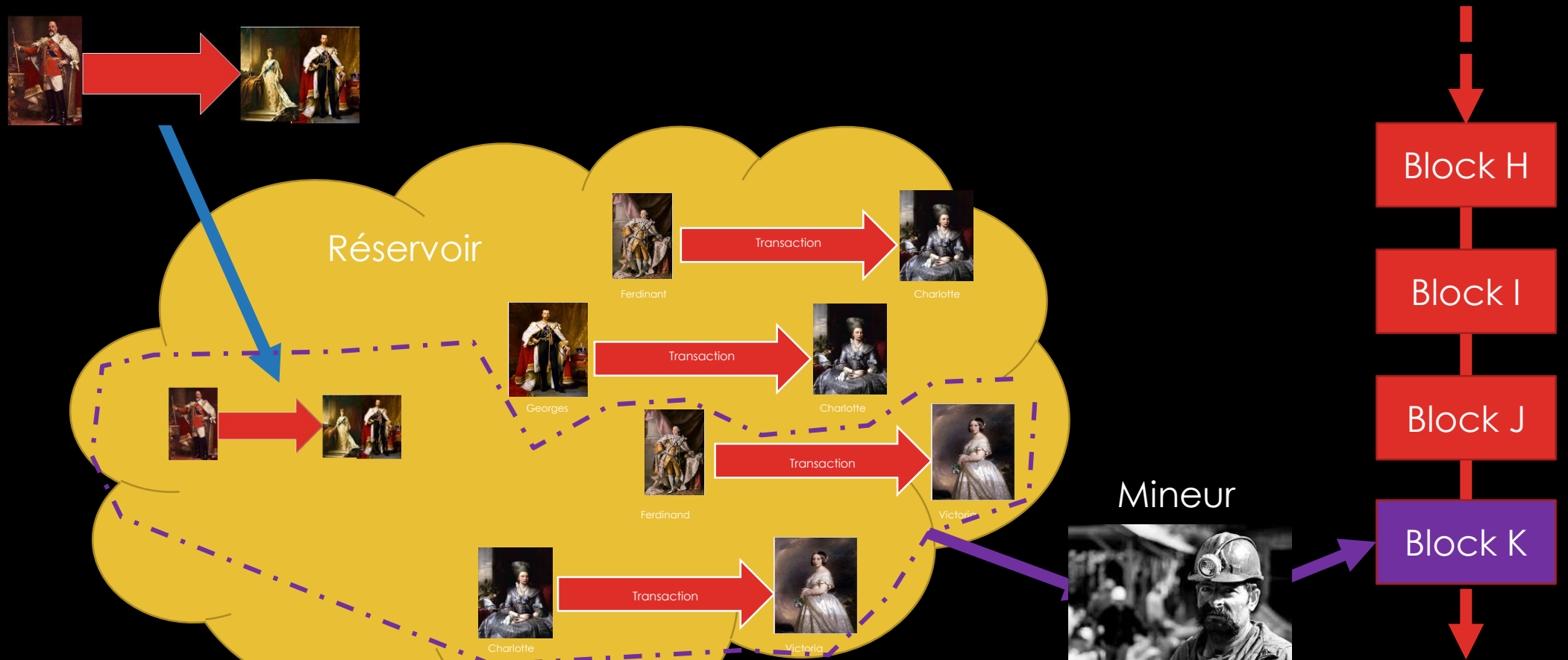
  => Chiffrement (encryption)

- Comment rendre une promesse officielle d'une manière numérique:

  => La chaine de block

CRÉATION D'UN BLOC

- Les transactions sont regroupées dans un bloc connecté au bloc précédent. C'est le rôle du mineur de faire cela.



RÔLE DU MINEUR

- Le mineur a un rôle clé:
  - Il / elle doit vérifier si la transaction est correcte
    - Garanti l'origine des «biens» en parcourant la chaine des blocs
    - Pour cela il/elle conserve l'entièreté du registre
  - Il/elle collecte les transactions pour les mettre dans un bloc
  - Qui devrait être incité à jouer correctement au jeu
  - À qui nous ne faisons pas confiance (a priori)

Pour respecter ces exigences, il y a 3 murs de protection:

- Le mineur est choisi au hasard dans une communauté de mineurs
- D'autres mineurs approuvent le travail effectué en ajoutant le bloc nouvellement créé à leur propre blockchain
- Seule la blockchain la plus longue est valide

Consensus

CHOIX D'UNE BLOCKCHAIN

1. Besoin de partager une base de données commune et toujours à jour
2. Impliquant plusieurs acteurs/parties
3. Les parties impliquées ont des intérêts divergents et/ou ne sont pas dignes de confiance et/ou risque d'être attaquées (cyber)
4. Les règles qui régissent les participants sont identiques et ne changent pas régulièrement
5. Besoin d'un archivage immuable

Alors une blockchain est la solution

Soit via une chaine de bloc privée (Axa, Bosch, IBM …) =>proof of stake

soit via une chaine de bloc public => proof of work

SECTEUR DE L'ENERGIE

Quelques exemples

- Solarcoin
  - Actif numérique (token appelé SLR) créé comme un moyen de récompenser la production d'électricité solaire mondiale
  - Les propriétaires de PV reçoivent 1 SLR / MWH
  - SLR peut être échange avec d'autres devises crypto ou $ - € (0,28 $ / SLR en avril 2018)
  - C'est une crypto monnaie

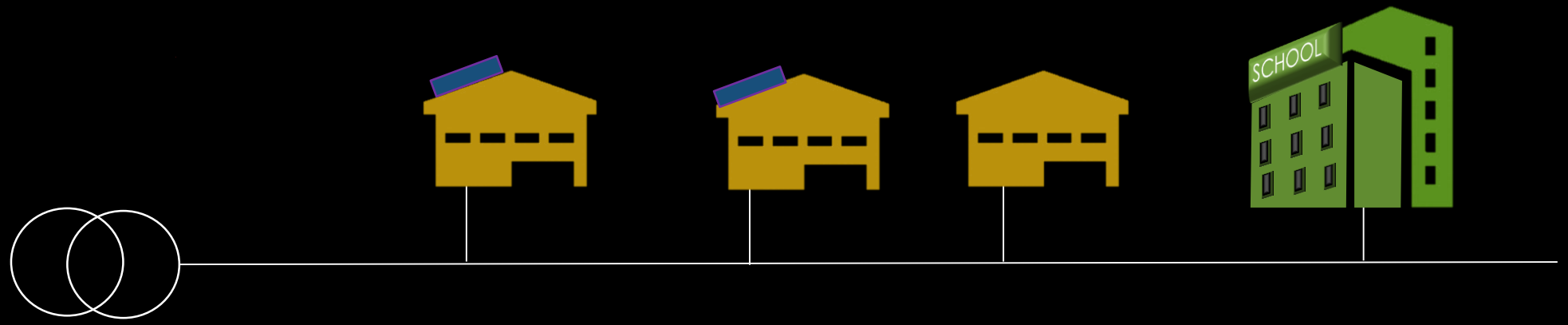
SECTEUR DE L'ENERGIE

Quelques exemples

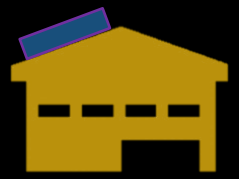
- Conjoule
  - Leur premier service est un marché local de l'énergie qui permet à Providing Homes (maisons productrices d'énergie renouvelable) de vendre leur surplus d'énergie directement aux foyers et organisations locaux.
  - 2 pilotes à Kettwig et à Mülheim (Allemagne)
  - Parmi les premiers consommateurs d'énergie pour le pilote, il y a une école, le, et une compagnie d'eau
  - Les prosommateurs peuvent choisir librement, quel consommateur ils veulent fournir avec leur surplus d'énergie générée.

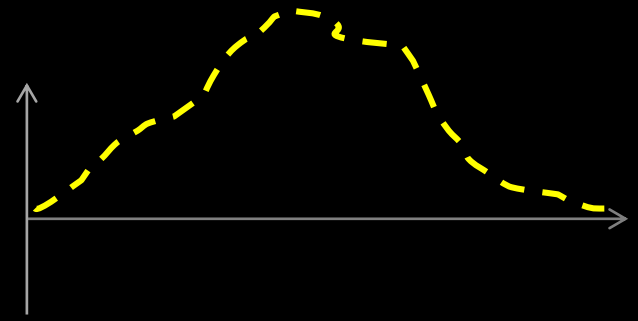
SECTEUR DE L'ÉNERGIE

- Echange d'énergie

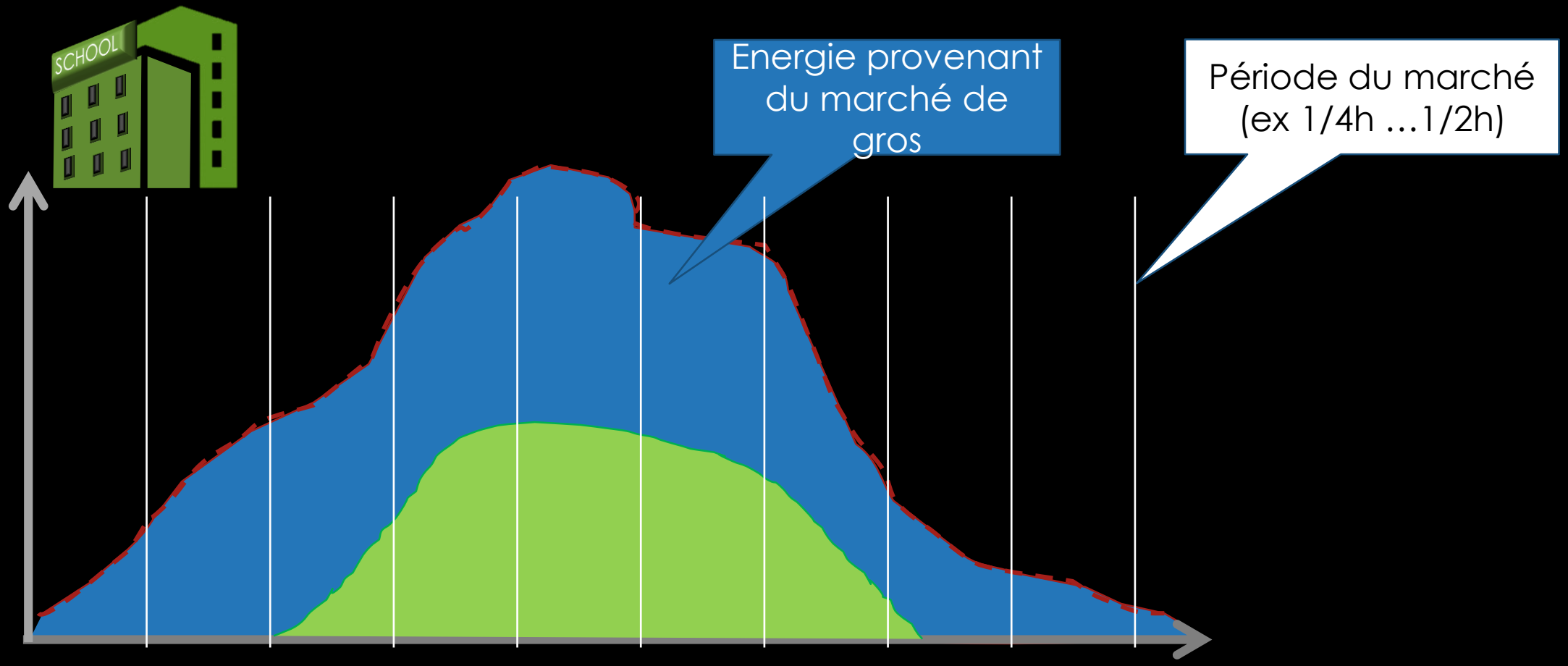


SECTEUR DE L'ÉNERGIE

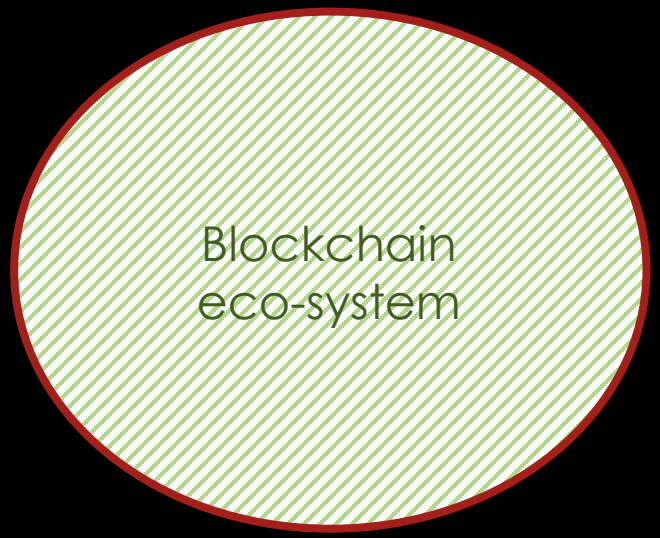




SECTEUR DE L'ÉNERGIE

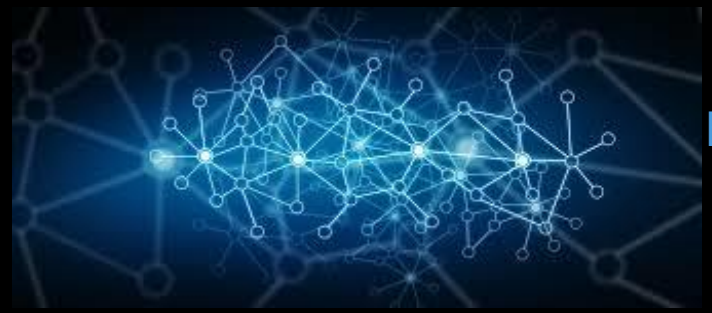


SECTEUR DE L'ÉNERGIE



SECTEUR DE L'ÉNERGIE

- Un tel mécanisme devrait garantir:
  - Précision et fiabilité des mesures
  - Traçabilité des échanges
  - Respect de la vie privée: c'est-à-dire offrir une défense suffisante pour qu'une attaque externe ne puisse accéder à des informations personnelles
  - Scinder parfaitement les échanges "paire à paire" avec ce qui vient du marché (sur la même base de temps)
  - Donner au marché et/ou au client de l'information proche du temps réel.



Est-ce que la blockchain répond à ces exigences?

Oui, sauf les 4ième et 5ième exigences, pourquoi ?

RÔLE DU MINEUR

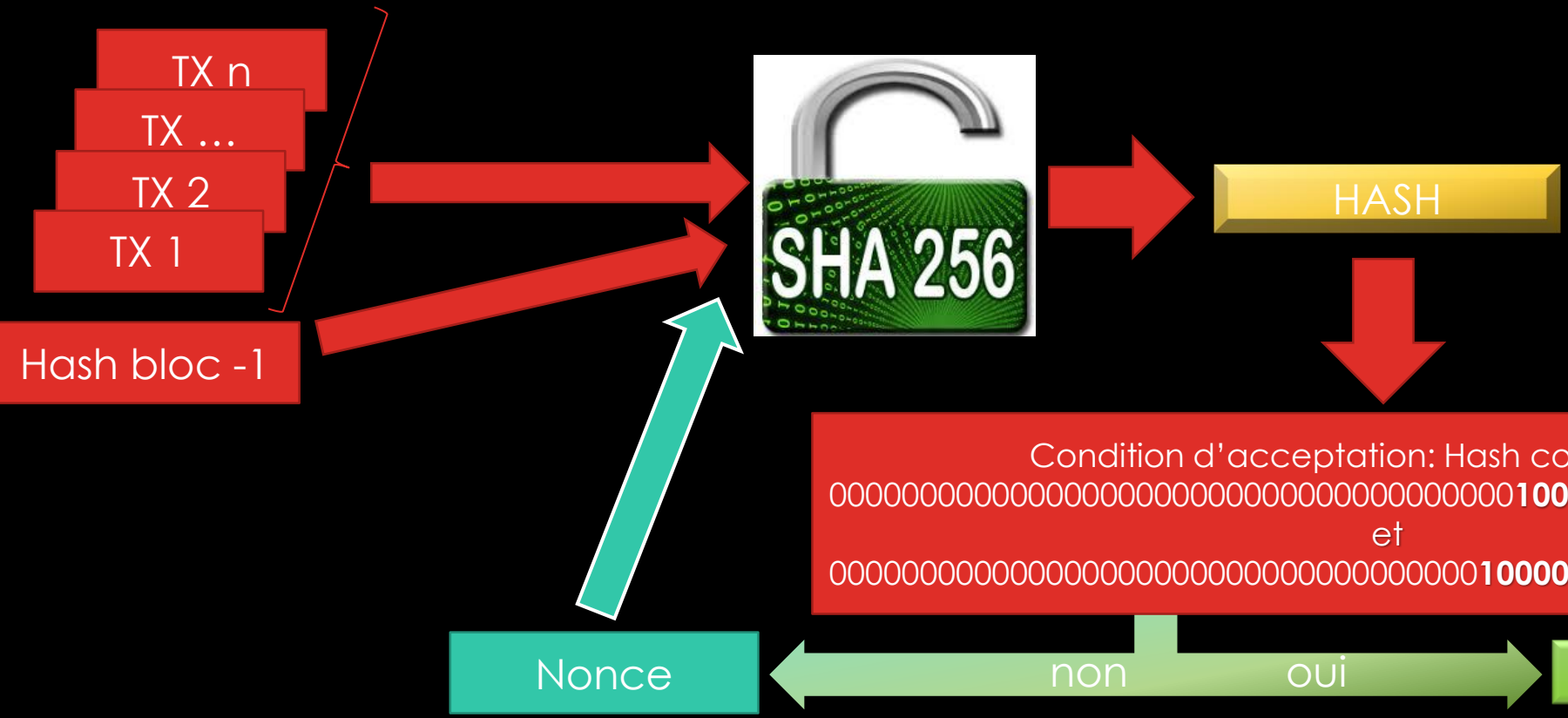
- Le mineur met de la puissance de calcul et l'espace de mémoire disponible à une communauté pour soutenir une chaîne de blocs
- Mais comment les motiver et comment les sélectionner "au hasard"?
- Il y a 2 façons
  - «Preuve d'enjeu» (proof of stake)
  - «Preuve de travail» (proof of work)

PREUVE DE TRAVAIL

- Principe
  - Résoudre un puzzle mathématique sans connaître l'image de départ
  - Lorsque le mineur réussit, il reçoit une incitation (par exemple 12,5 Bitcoin sont créés) en plus des frais de transaction
- Avantages
  - Simple à mettre en œuvre
  - Très efficace quand les mineurs sont de parfaits inconnus
- Désavantages
  - Enorme consommation d'énergie
  - Encourage la création d'équipements spécifiques (pas plus dans la philosophie d'utilisation des équipements existants)
  - La probabilité de succès (création d'un bloc) est une moyenne par ex. toutes les 10 minutes
  - La validation est créé sur base de la chaine la plus longue. Donc il faut attendre un certain nombre de bloc (par ex 6)

PREUVE DE TRAVAIL

- Comment ça fonctionne= chiffrement par le Hash



PREUVE D'ENJEU

- Principe
  - Désigné au hasard
  - Au plus un mineur a des intérêts dans la chaine (stake), au plus il est susceptible d'être sélectionné
- Avantages
  - Peu énergivore
  - Particulièrement efficace quand les mineurs sont à priori de confiance (p.ex font partie de la même entreprise)
- Inconvénients
  - Comme il n'est pas très couteux de faire un bloc, le mineur peut être tenté de suivre plusieurs chaines à la fois (affaibli le consensus) =>Motivation des mineurs

PROPOSITION D'UNE CHAÎNE SYNCHRONISÉE

Selection done by last Miner

Voting token
- For each Tx a token E (of a given value) is created and is assigned to the transmitter (k)

Candidates Announcement
- Each candidate sends the #E that he/she is ready to use

Computation of the Stake/Wealth
- For each candidate =

$$\alpha E^{k}_{T_i-1} + \beta A^{k}_{T_i-1} + \gamma R^{k}_{T_i-1} i$$

Generation of random numbers
- For each candidate Uk between]0;1]

Selection of the best k
- Winner = k with arg max Wk / Uk
- He/she receives all the voting token sent by candidates

A = Age of the last block created by the candidate
R = reputation of the candidate (e.g. # of her/his block in the main chain)

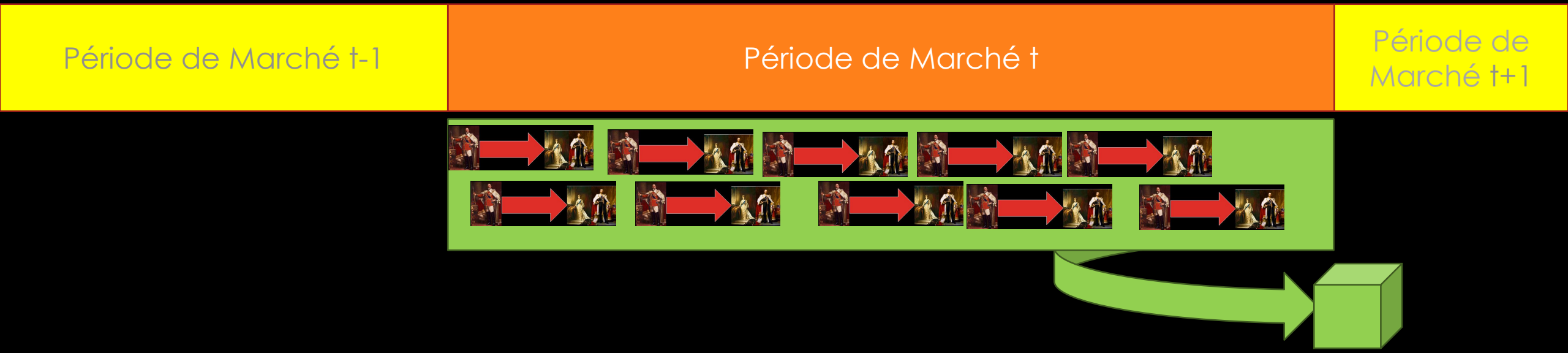
PROPOSITION D'UNE CHAÎNE SYNCHRONISÉE

Chaque candidat envoie un nombre de jetons de vote au mineur actuel.
La période de vote:

- commence un petit moment après le début de la période de marché (afin d'avoir le temps de diffuser le gagnant de cette période de marché)
- et se termine avant la période de marché (afin de régler le processus de sélection)

PROPOSITION D'UNE CHAÎNE SYNCHRONISÉE

Chaque candidat forge un bloc avec toutes les transactions effectuées pendant la période de marché et le diffuse



PROPOSITION D'UNE CHAÎNE SYNCHRONISÉE

- Le **consensus** est créé par:
  - Tous les nœuds (candidats ou non) ajoutent le bloc du vainqueur à leur propre chaîne si ce bloc est égal à la majorité des bloc des différents candidats
  - Ceci est transparent et donc vérifiable par tous les nœuds.
  - La chaîne la plus longue correspond à la «vérité».
- Le bloc contient toutes les transactions d'une période de marché et est compatible avec le marché de gros.
- La motivation du mineur est liée à la valeur du jeton de vote
- La validation du bloc est le temps entre la fin de la période de marché et l'ouverture aux candidatures du bloc suivant.

CONCLUSION

- Le mécanisme proposé répond aux exigences:
  - Précision et fiabilité des mesures
  - Traçabilité des échanges
  - Respect de la vie privée: c'est-à-dire offrir une défense suffisante pour qu'une attaque externe ne puisse accéder à des informations personnelles
  - Scinder parfaitement les échanges "paire à paire" avec ce qui vient du marché (sur la même base de temps)
  - Donner au marché et/ou au client de l'information proche du temps réel.