ADN Numérique Responsable

Journée du Numérique Responsable dans l'Ouest

25 janvier 2022 - Angers

Partagez votre expérience : #JNR2022

@adnouest

Comment allier sécurité informatique et numérique responsable ?

Partagez votre expérience : #JNR2022

@adnouest

Karim Zkik

ESAIP

Enseignant-chercheur en Cybersécurité & Réseaux

Blockchain : de la recherche à l'innovation en entreprise

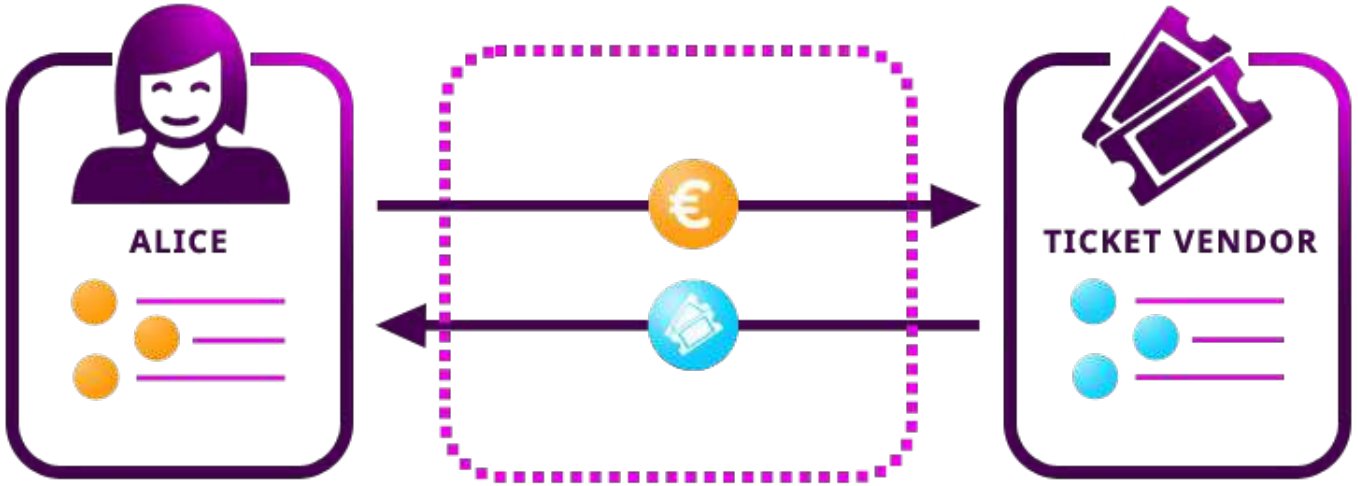
KARIM ZKIK

La journée du Numérique Responsable dans l'Ouest,
25 Janvier 2022

Les Transactions

Pour créer une transaction valide

- Vous devez d'abord prouver la propriété de ce que vous voulez échanger
- Vous devez connaître le destinataire
- L'expéditeur doit signer



Les Transactions : Modèle Classique (ou Centralisé)

Une manière «classique» de faire une transaction:

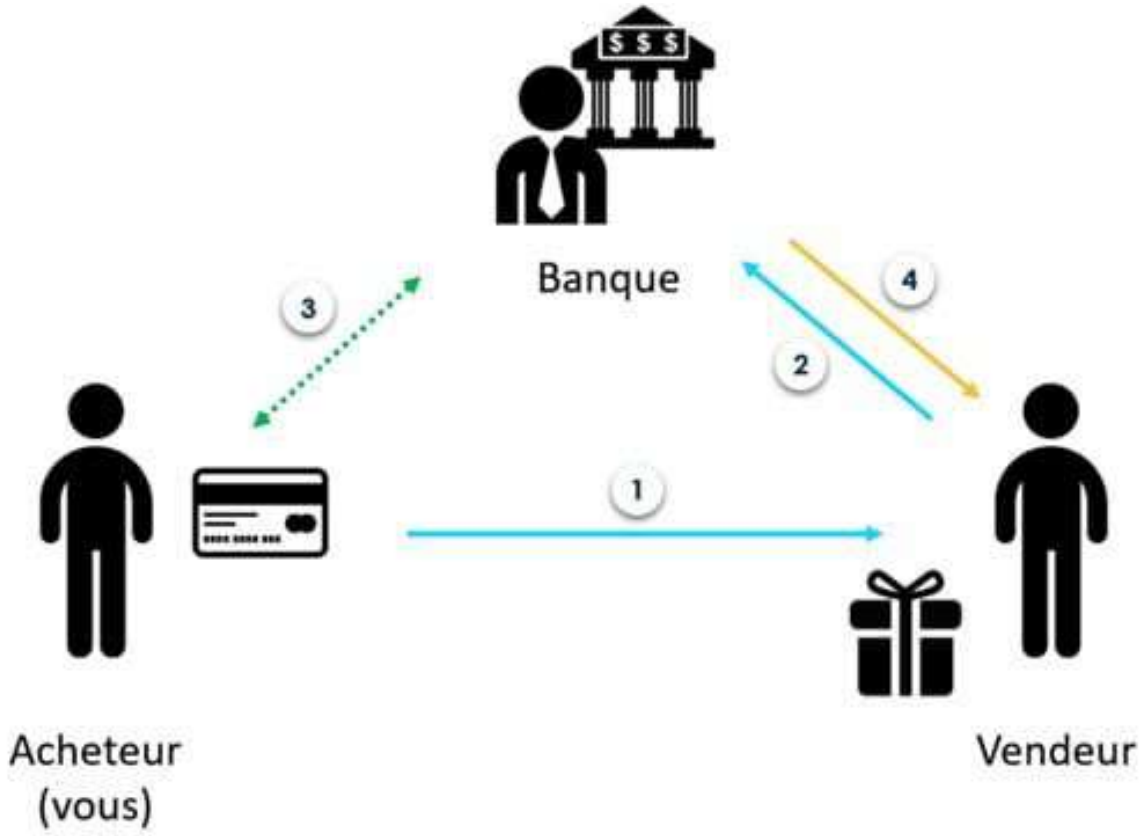
Faire confiance a une autorité (légale) pour que les transactions sont correctement signées, vraies et authentique.

Cette autorité est nommée l'homme au milieu (Notaire - Banque - société de lecture de compteurs ...)

"L'homme au milieu" enregistre ces transactions dans un livre, un grand registre ou une base de données.

Blockchain

Les Transactions : Modèle Classique (ou Centralisé)



1. Vous souhaitez régler un achat de 100€ par carte bancaire. Vous insérez votre CB dans le terminal de paiement du marchand et saisissez votre code
2. Le vendeur (par le biais du terminal) interroge votre banque pour savoir si vous avez bien 100€ sur votre compte.
3. Votre banque vérifie que vous avez au moins 100€ sur votre compte
4. Votre banque confirme que vous avez bien 100€ et valide la transaction.

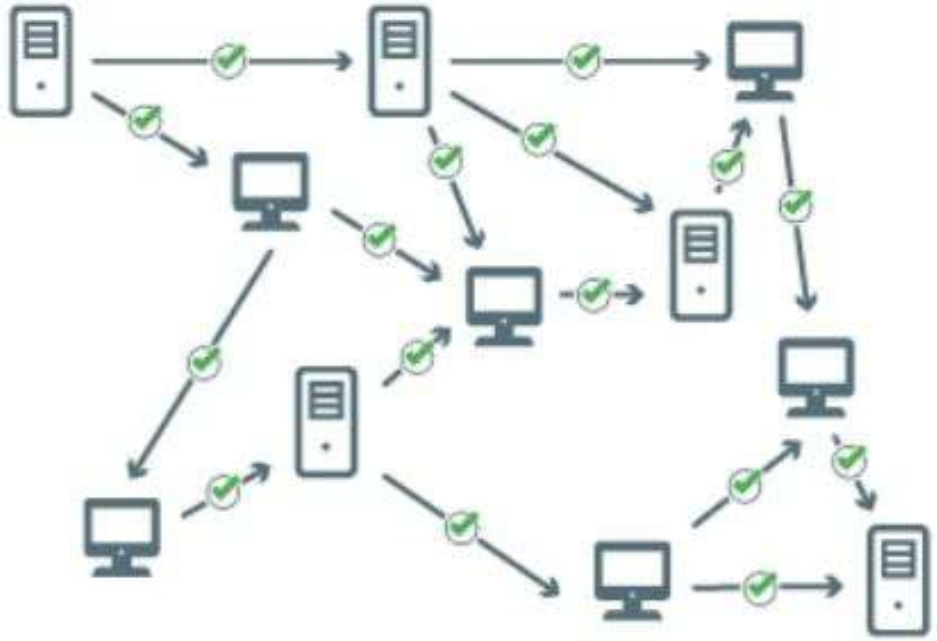
Les Transactions : Limites du Modèle Classique

- Il faut faire Confiance «l'homme au milieu»
- Le temps de la transaction
- Frais de transactions
- Le respect de la vie privée
- Complexité des procédures
- Risque d'altération / de triche des enregistrements
- Risque de manipulation / destruction du registre

Les Transactions : La décentralisation

Une application décentralisée, est une application qui fonctionne sur un réseau décentralisé, par opposition aux applications classiques qui reposent sur des serveurs centralisés.

La décentralisation des transactions permet de faire des échanges sans organe central de contrôle. Autrement dit, sans aucune autorité pour l'émettre, la réguler ou la contrôler (régulateurs), et ce, sans intermédiaires assurant ses transactions (banques)



Les Transactions : Défis de la décentralisation

- Comment prouver la propriété de ce que vous voulez échanger ?
- Comment connaître et échanger avec le destinataire?
- Comment assurer l'authenticité de ce que vous vous échanger?

Blockchain : Origines

Le 31 octobre 2008, **Satoshi Nakamoto** a publié le papier **Bitcoin: A Peer-to-Peer Electronic Cash System** décrivant un système de transfert de trésorerie / d'actifs numériques purement peer to peer. Il s'agit de la première implémentation populaire de Blockchain et est attribuée comme étant la naissance de l'industrie Blockchain d'aujourd'hui.

Blockchain : La notion de Bloc

Les transactions effectuées entre les utilisateurs du réseau sont regroupées par ce qu'on appelle **un bloc**. Chaque bloc est validé par les nœuds du réseau appelés les **mineurs** selon des techniques qui dépendent du type de blockchain.

Un bloc est constitué de:

- index,
- timestamp,
- hash,
- previous hash,
- data,
- nonce.

Le premier bloc est nommé Genesis Block

Genesis Block	
Previous Hash	0
Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
Data	Welcome to Blockchain CLI!
Hash	0000018035a828da0…
Nonce	56551

Blockchain : Comment ça marche

Une blockchain est une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création.

Selon la **Banque de France** ses principales caractéristiques sont:

- **L'identification** de chaque partie s'effectue par un procédé cryptographique

- **La transaction est envoyée à un réseau (ou « nœud » de stockage)** d'ordinateurs situés dans le monde entier. chaque « nœud » héberge une copie de la base de données dans lequel est inscrit l'historique des transactions effectuées.

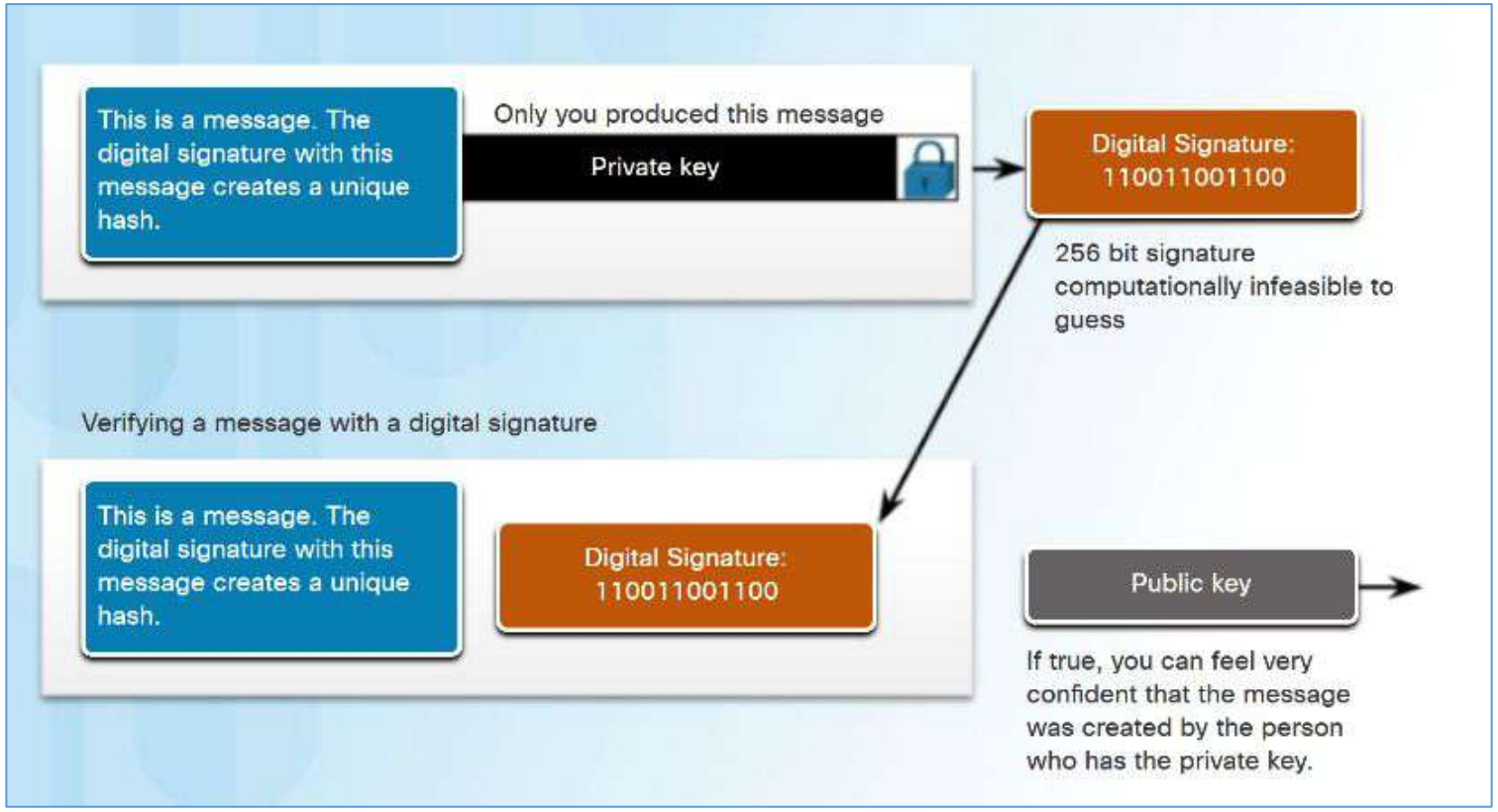
- **Un mécanisme de consensus** de tous les « nœuds » à chaque ajout d'informations. Les données sont déchiffrées et authentifiées par des « centres de données». La transaction ainsi validée est ajoutée dans la base sous forme d'un bloc de données chiffrées (c'est le « block » dans blockchain)

La décentralisation de la gestion de la sécurité empêche la falsification des transactions. Chaque nouveau bloc ajouté à la blockchain est lié au précédent et une copie est transmise à tous les « nœuds » du réseau.

Blockchain : Procédure

Identification: Signatures numériques

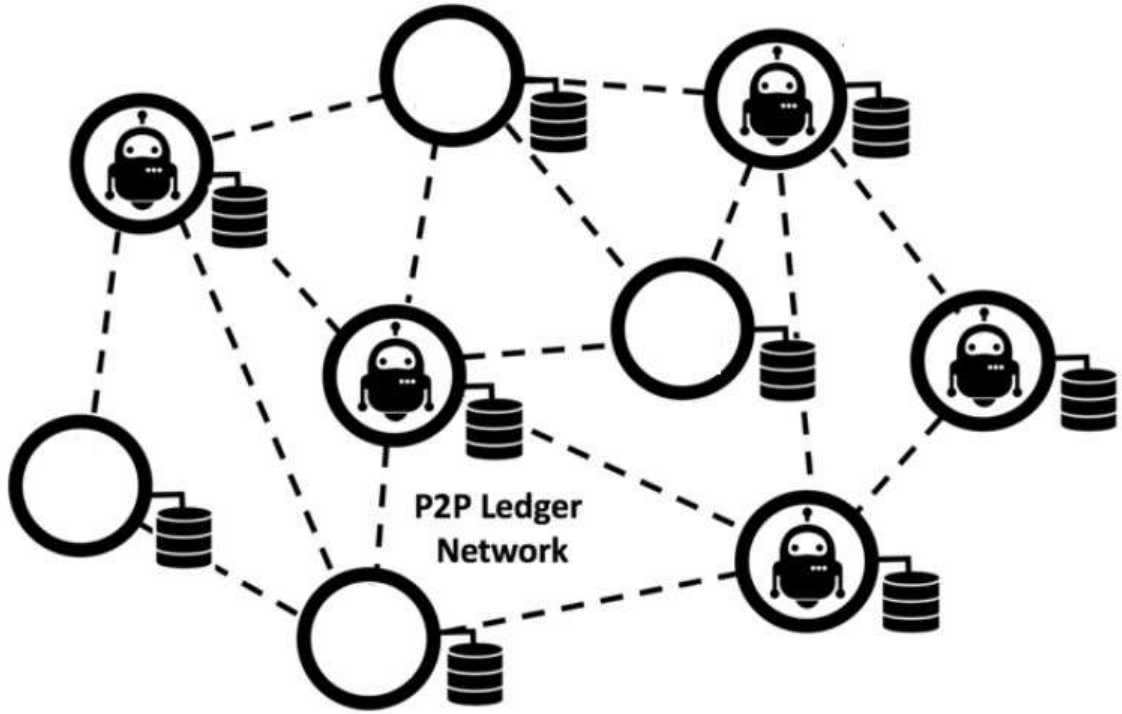
- Une signature numérique est un schéma mathématique permettant de démontrer l'authentification d'informations numériques.
- Changer le message, même légèrement, rend la signature numérique complètement différente.



Blockchain : Procédure

Grand registre (base de données) décentralisé

- Blockchain utilise un registre décentralisé avec toutes les parties intéressées en conservant une copie.
- La confiance est assurée par tous ceux qui reçoivent et croient à toute nouvelle transaction.
- Tout le monde doit utiliser et travailler avec exactement le même registre. Cela se fait à l'aide d'un processus appelé preuve de travail.



Blockchain : Procédure

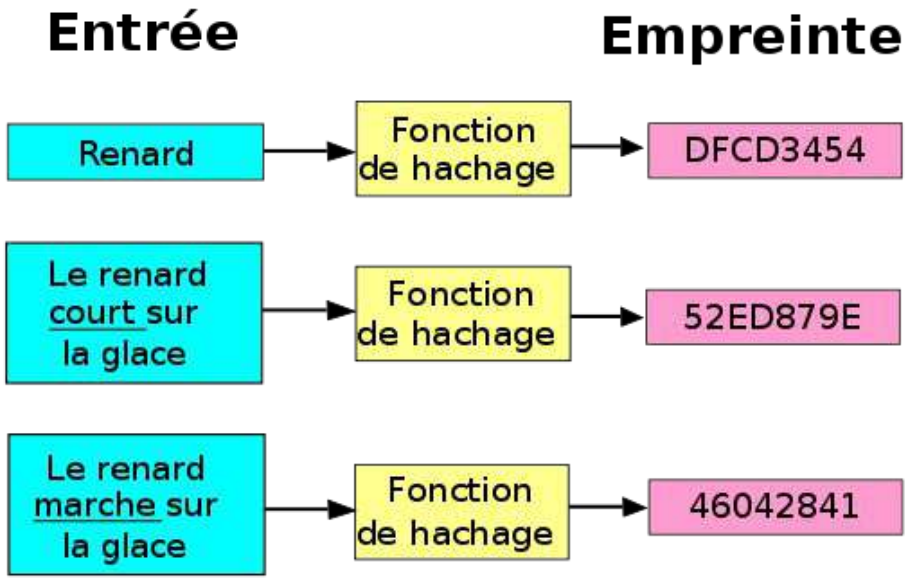
Atteindre un consensus

- Un bloc comprend les transactions ainsi que leurs signatures numériques. La validation des transactions dans un bloc utilise un processus appelé Proof of Work (PoW).
- **Le PoW est un algorithme (hachage) exécuté** par des ordinateurs **(les mineurs)** qui nécessite une grande quantité de travail de calcul dans un laps de temps relativement court.
- Une blockchain se compose de blocs. Chaque bloc est une liste de transactions, avec un hachage du bloc précédent et un hachage de ce bloc, y compris son PoW.
  - Le hachage est calculé en utilisant le hachage du bloc précédent (PoW précédent), ainsi que toutes les transactions de ce bloc avec leurs signatures numériques.

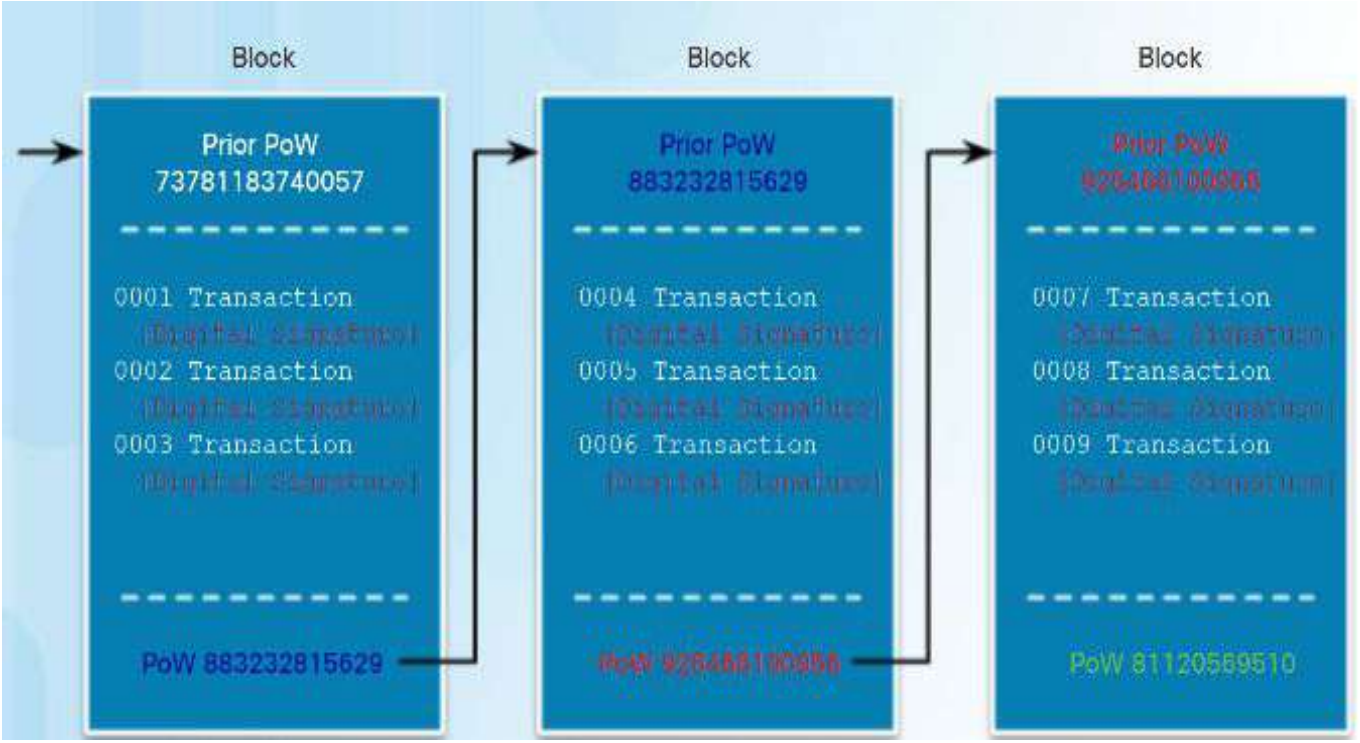
Cela rend impossible, d'un point de vue informatique, de modifier un bloc ou de changer l'ordre des blocs.

Blockchain

Blockchain : Procédure



Atteindre un consensus



Démo:

https://andersbrownworth.com/blockchain/blockchain

Blockchain

blockchain features

01. resistant to collusion

aucune autorité centrale ou élite suprême ne peut prendre de décisions unilatérales

02. fault tolerant

pas de serveur central donc le réseau est plus résistant aux pannes.

03. digital signatures

alice ne peut pas envoyer un message à bob et ensuite nier l'avoir jamais envoyé

04. resistant to modification

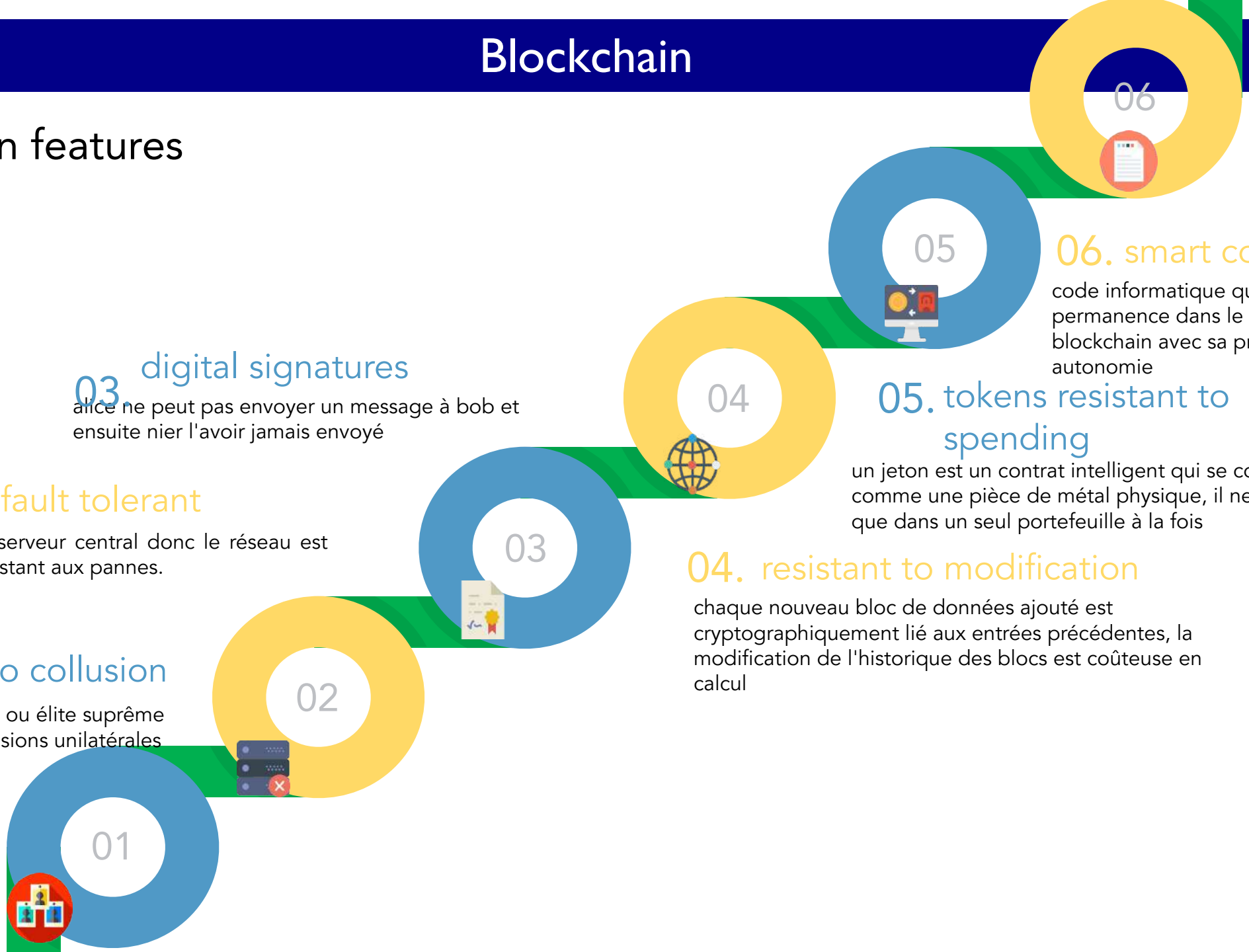
chaque nouveau bloc de données ajouté est cryptographiquement lié aux entrées précédentes, la modification de l'historique des blocs est coûteuse en calcul

05. tokens resistant to double spending

un jeton est un contrat intelligent qui se comporte comme une pièce de métal physique, il ne peut être que dans un seul portefeuille à la fois

06. smart contracts

code informatique qui s'exécute en permanence dans le réseau blockchain avec sa propre autonomie



Blockchain : Avantages

L'utilisation de la blockchain comporte de nombreux avantages, parmi lesquels :

- Favoriser la transparence
- la rapidité des transactions
- la sécurité du système,
- se prémunir du risque de malveillance ou de détournement,
- les gains de productivité et d'efficacité

Blockchain : Applications

- ✔ **Dans le secteur bancaire**, la technologie ouvre la possibilité de valider des transactions sans l'intermédiaire d'une chambre de compensation, ce qui devrait permettre de certifier des opérations dans des délais beaucoup plus courts.
- ✔ **Dans le secteur de l'assurance**, l'apport de la blockchain tient par exemple à l'automatisation des procédures de remboursement et à l'allégement de certaines formalités à la charge des sociétés comme de leurs clients
- ✔ **Dans le secteur de la logistique**, la blockchain présente deux intérêts : assurer une traçabilité des produits, ainsi que la mémoire des différentes interventions sur une chaîne de production et de distribution ; alléger les formalités et créer les conditions d'une coopération entre les acteurs d'une filière
- ✔ **Dans le secteur agro-alimentaire** pour la traçabilité des aliments, particulièrement intéressante en cas de crise sanitaire

De nombreux autre secteurs sont potentiellement concernés par l'utilisation de la technologie blockchain : santé, immobilier, aéronautique, etc.

Blockchain

Blockchain : Entreprises qui ont transformer leurs industries en utilisant Blockchain

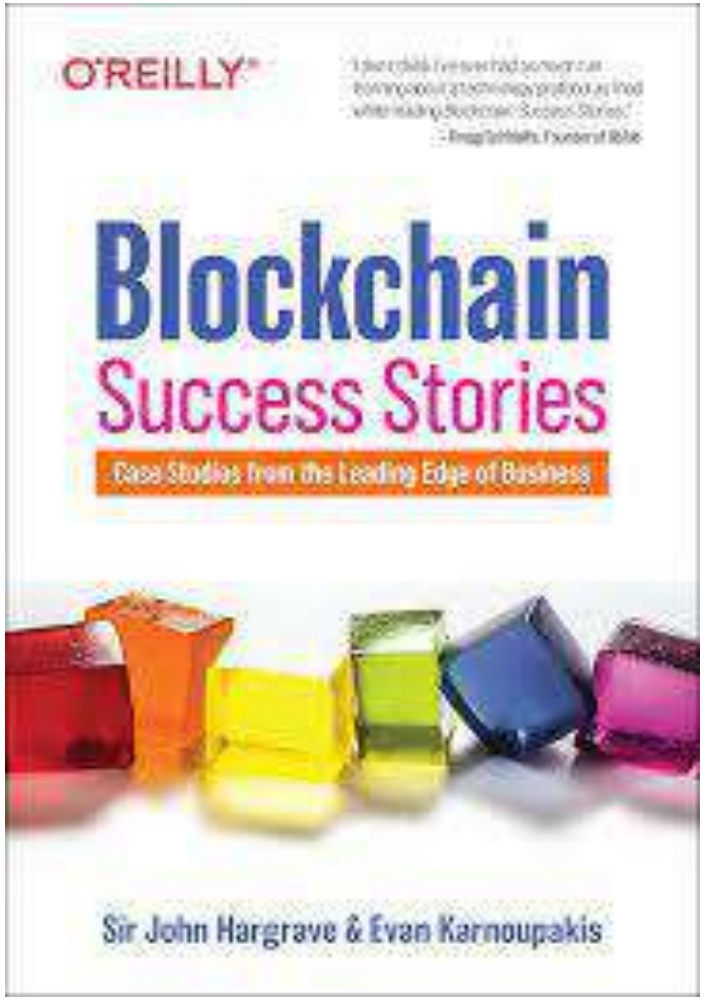
Nordea

inBlocks

Kroger

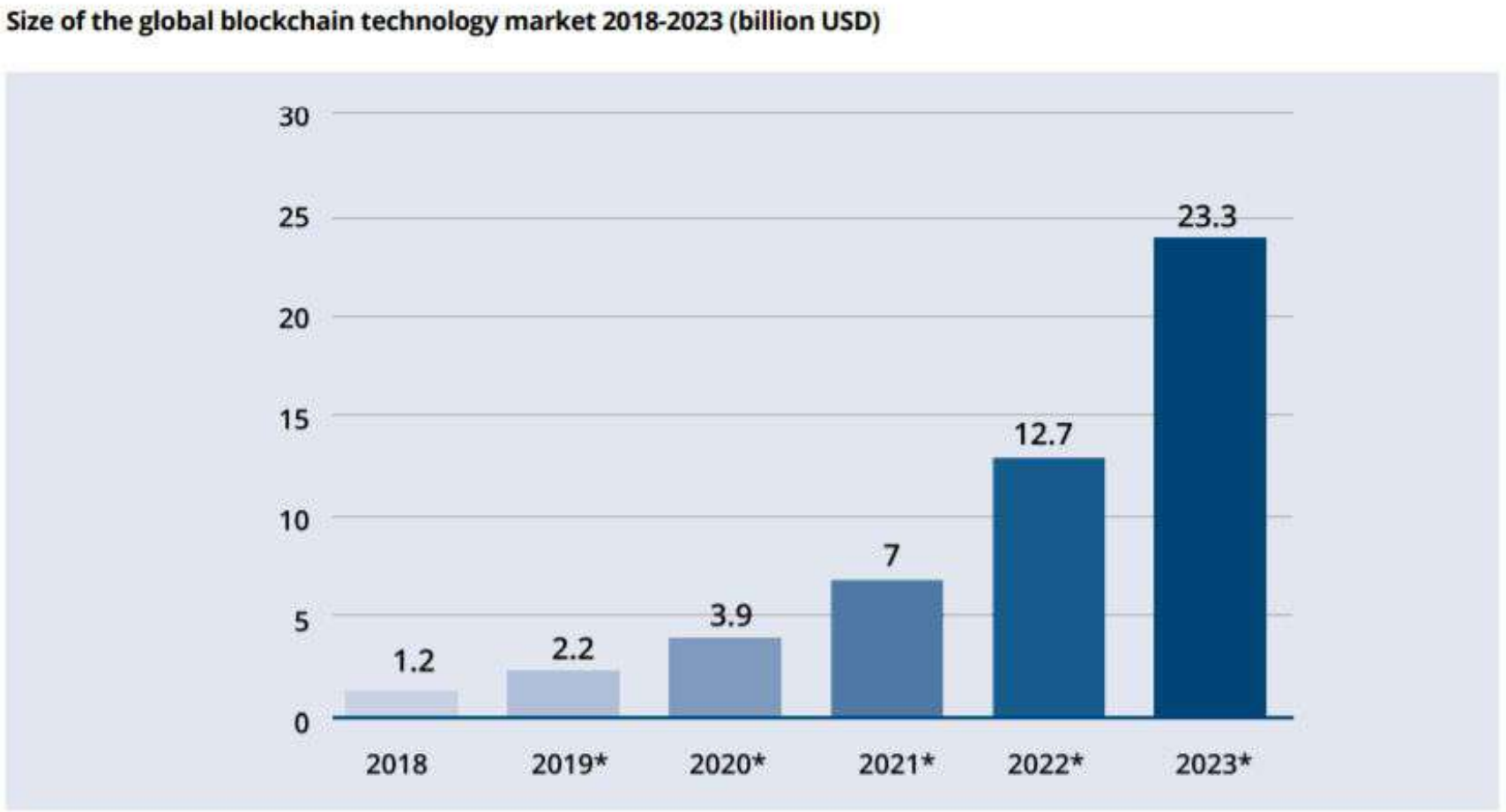
NuARCA
Establishing a World of Trust

plasticbank



Blockchain

Blockchain investment



Les barrières de l’adoption de la Blockchain

Obstacles liés à la gouvernance

- Absence de politique gouvernementale de BT et de durabilité
- Absence de réglementation soutenant l'utilisation du BT dans la durabilité
- Non visibilité sur la fiscalité
- Concurrence sur le marché et incertitude

Les barrières de l’adoption de la Blockchain

Obstacles liés au management

- Manque d'engagement et de soutien de la direction
- Absence de stratégie durable basée sur BT
- Manque de ressources financières
- Mauvaise structure organisationnelle

Les barrières de l’adoption de la Blockchain

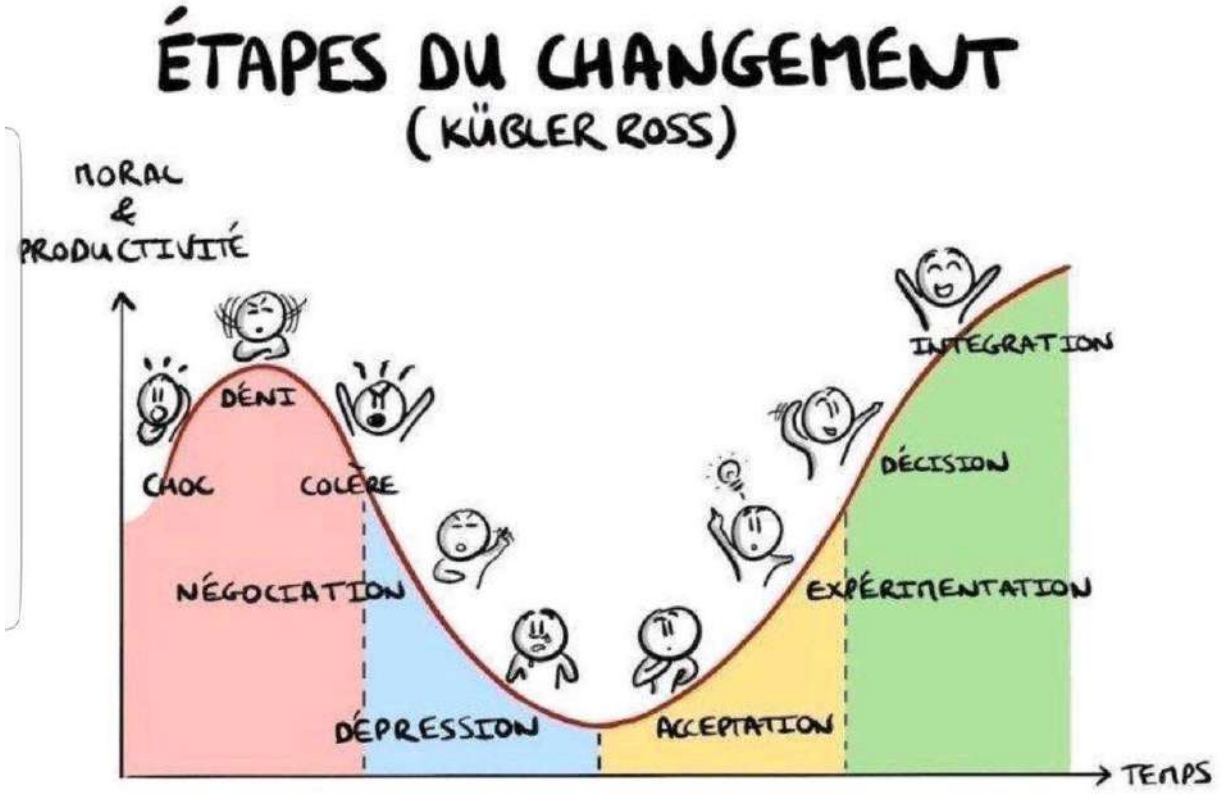
Obstacles liés aux technologies

- Problème de sécurité des données
- Infrastructure informatique médiocre
- Irréversibilité des transactions

Les barrières de l’adoption de la Blockchain

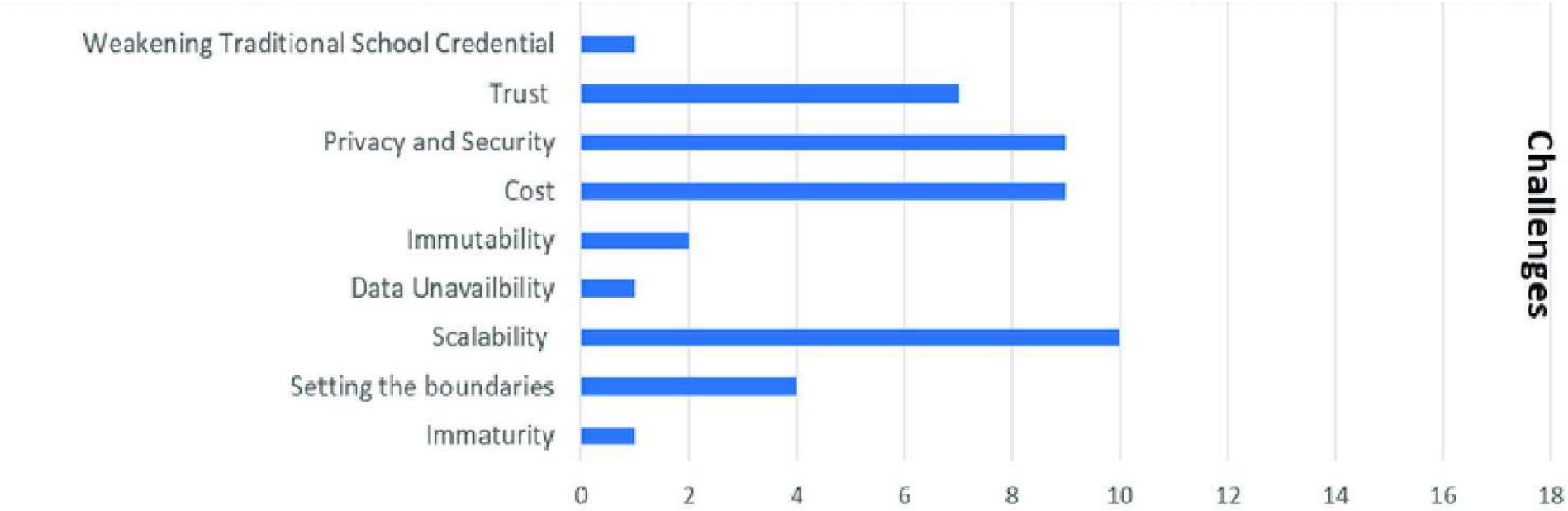
Obstacles liés aux ressources humaines

- Résistance au changement
- Manque d'expertise dans le domaine du numérique
- Non-disposition à la transparence
- Manque d'engagement des employés

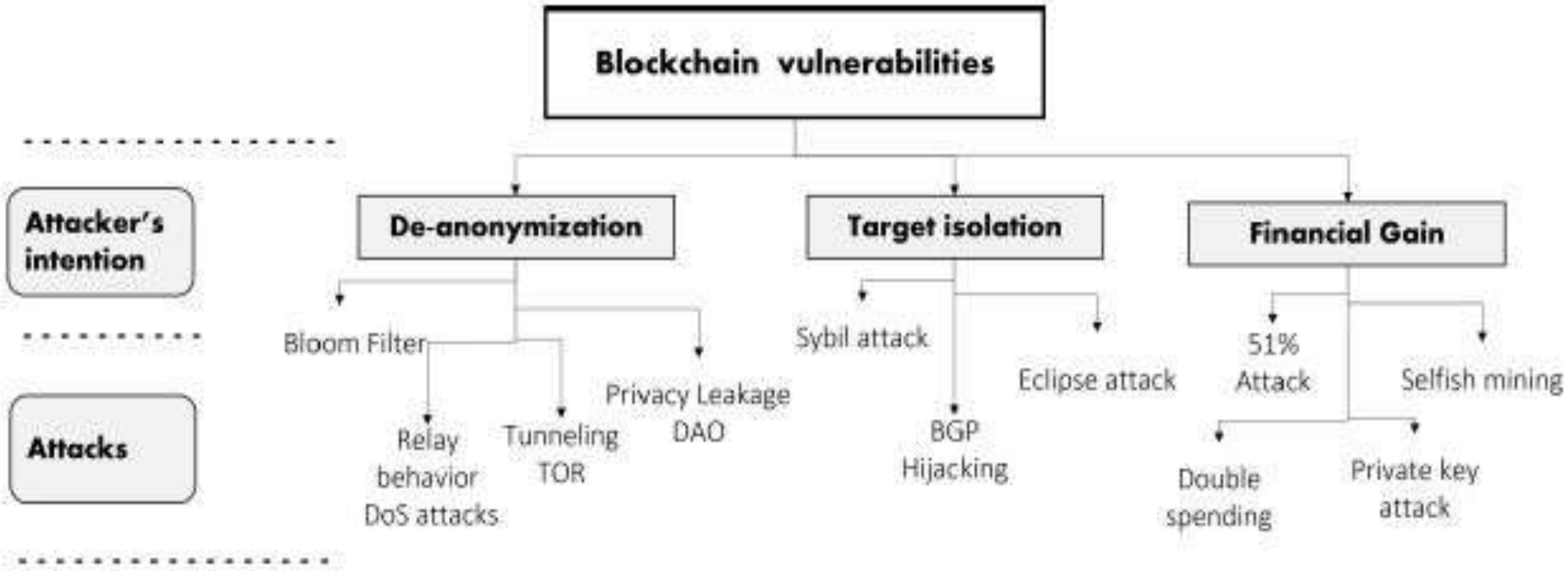


Blockchain

Les challenges de la Blockchain

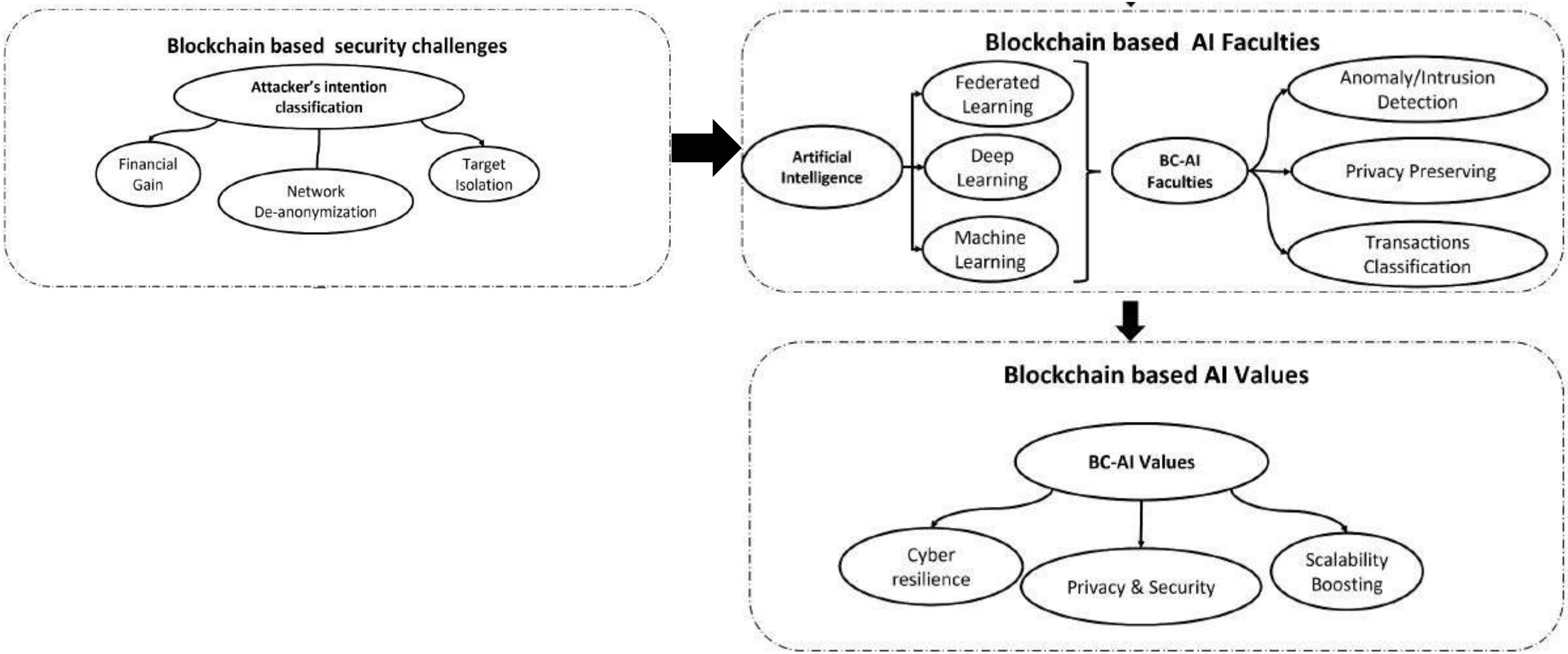


Sécurité des technologies Blockchain



Blockchain

AI leading the way to the security and privacy of Blockchain



Blockchain

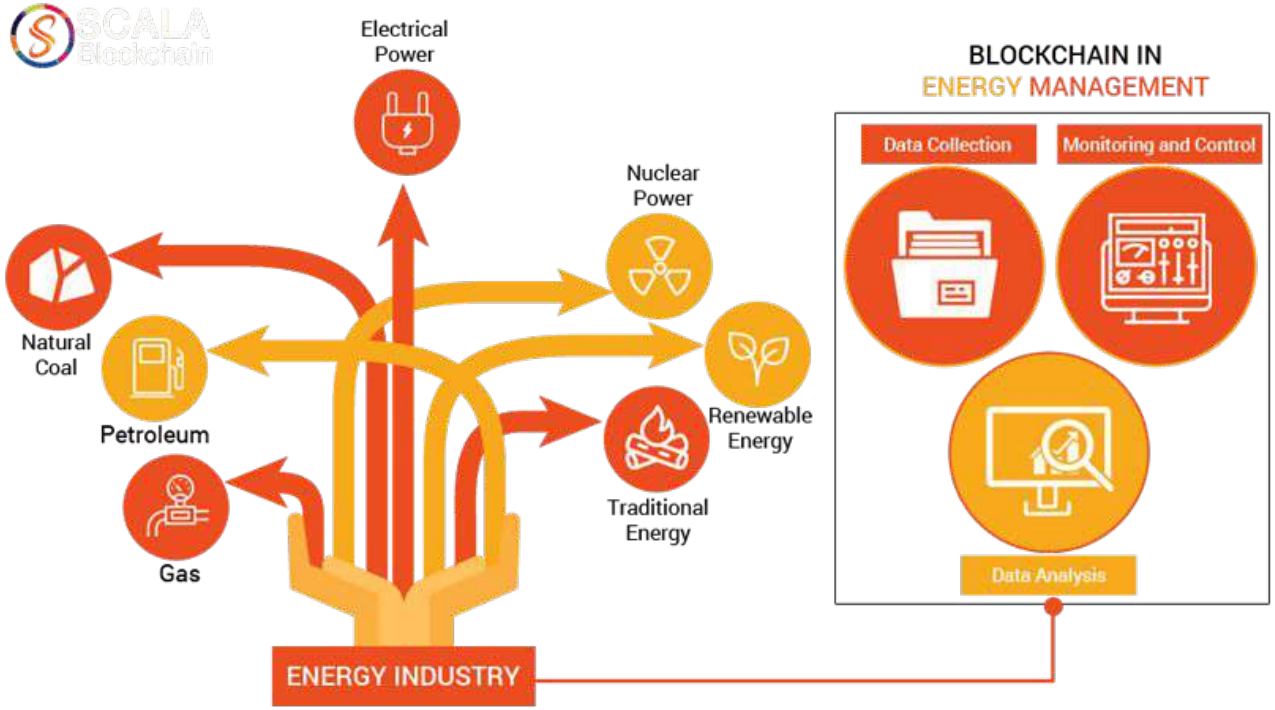
Blockchain for green

Negative Aspect

⇒ **Energy Consumption**

Positive Aspect

⇒ **Blockchain in the energy industry**



Blockchain : Energy Consumption

- Les opérations de vérification, de validation et de cryptographie consomment beaucoup d'électricité

- Une large diffusion des blockchains pourrait avoir un fort impact négatif sur l'environnement

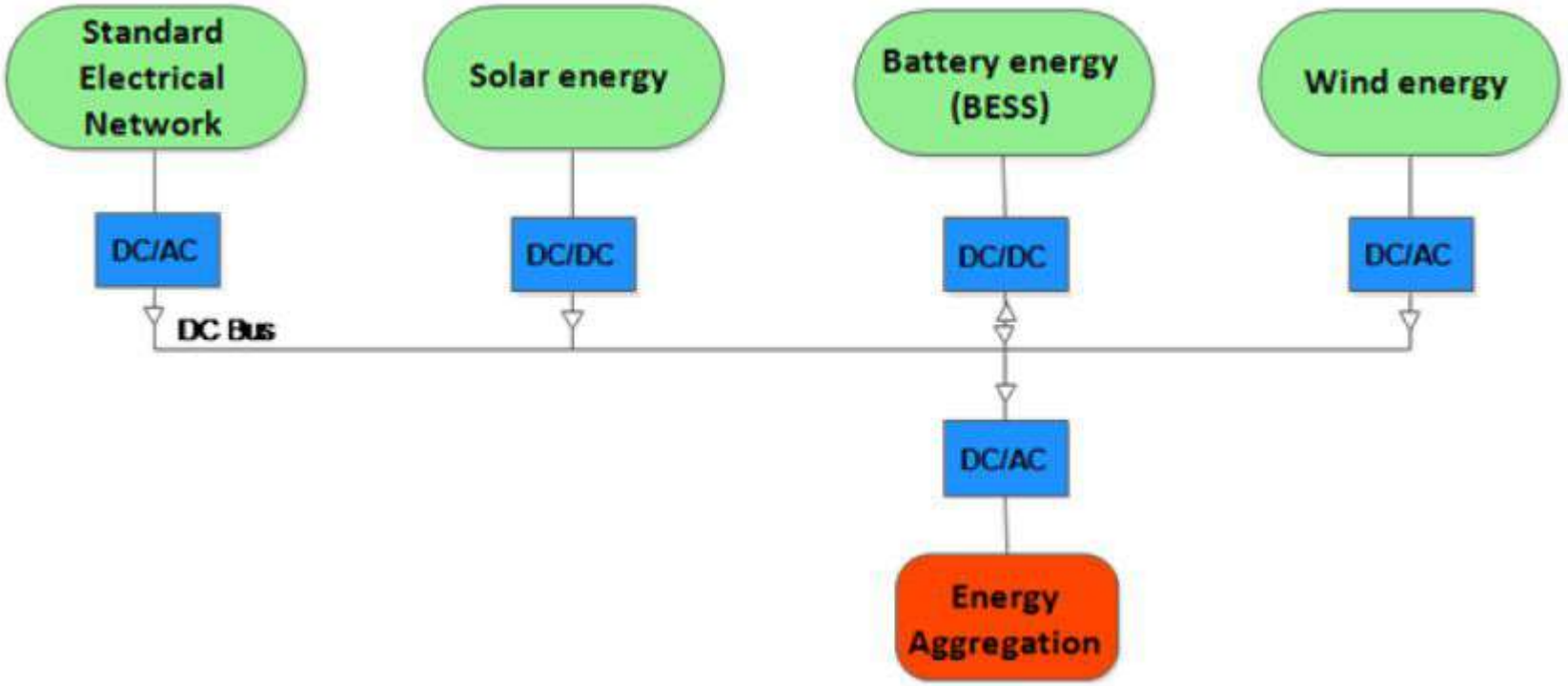
L'enjeu est ici de développer des solutions techniques moins coûteuses en énergie, mais avec les mêmes garanties en termes de sécurité et de transparence

Blockchain

Blockchain : Energy Consumption

Blockchain : Energy Consumption

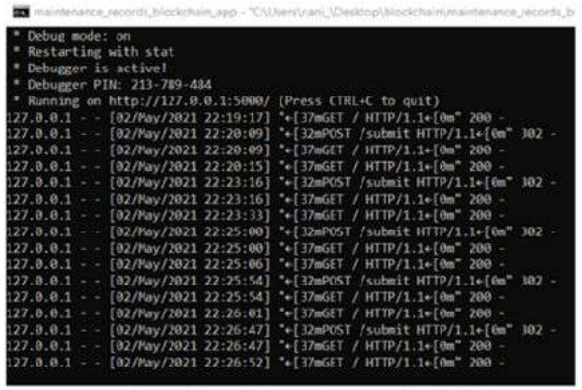
Projet d'optimisation des Micro-grid alimentant les centres de données Blockchain



Blockchain : Energy Consumption

Front end and back-end interface d'une blockchain adapté aux systems industriel

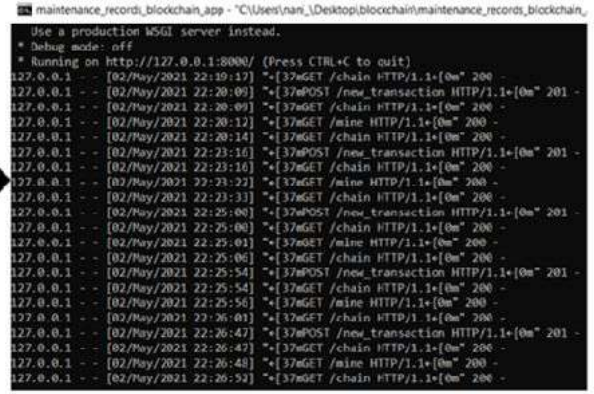
Back-end Trairement



Start a blockchain node server (POST/GET)

Consensus Pre-Traitement

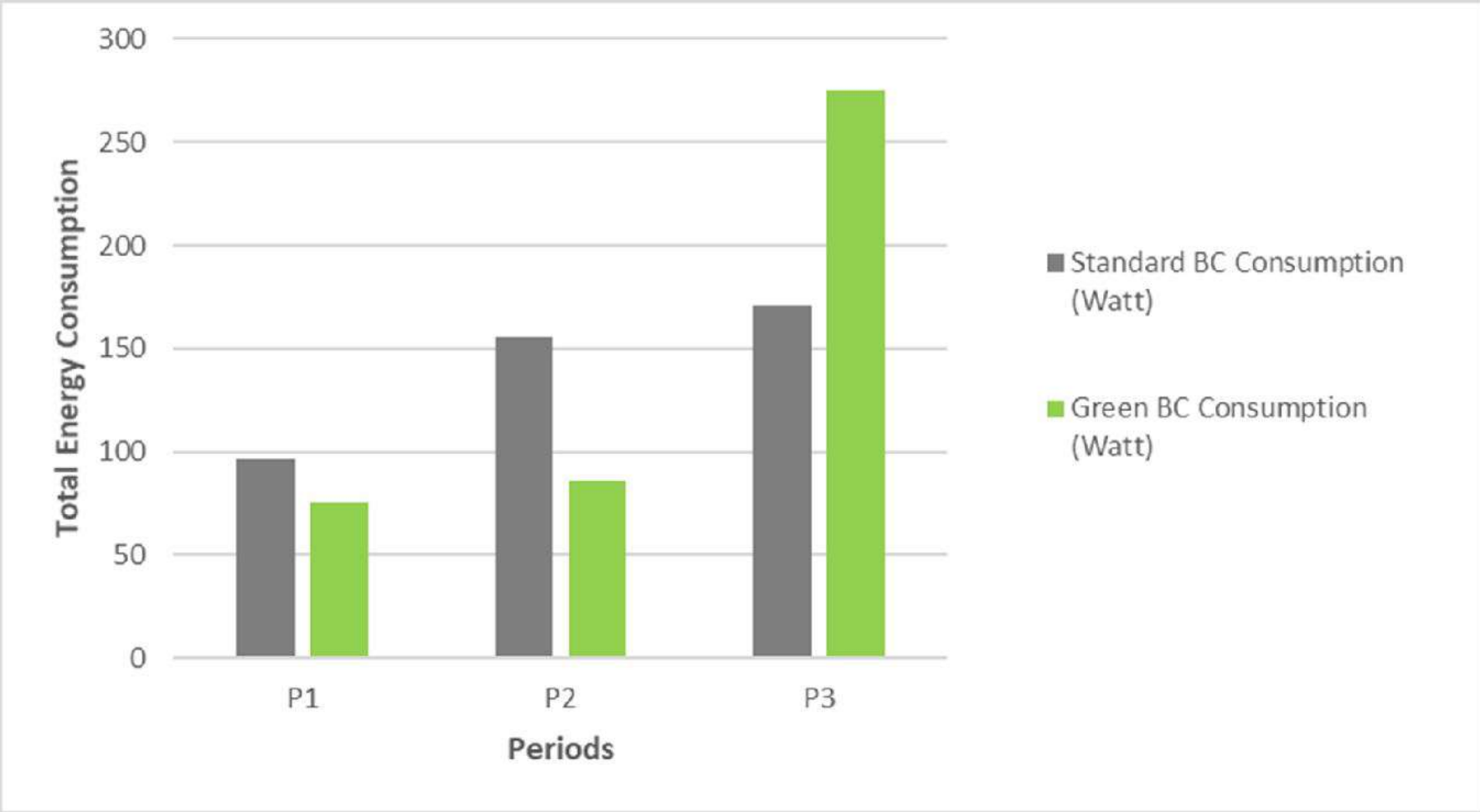
Requesting the node to mine



Checking if the proof is valid & add new transaction to the Blockchain

Blockchain : Energy Consumption

Front end and back-end interface d'une blockchain adapté aux systems industriel

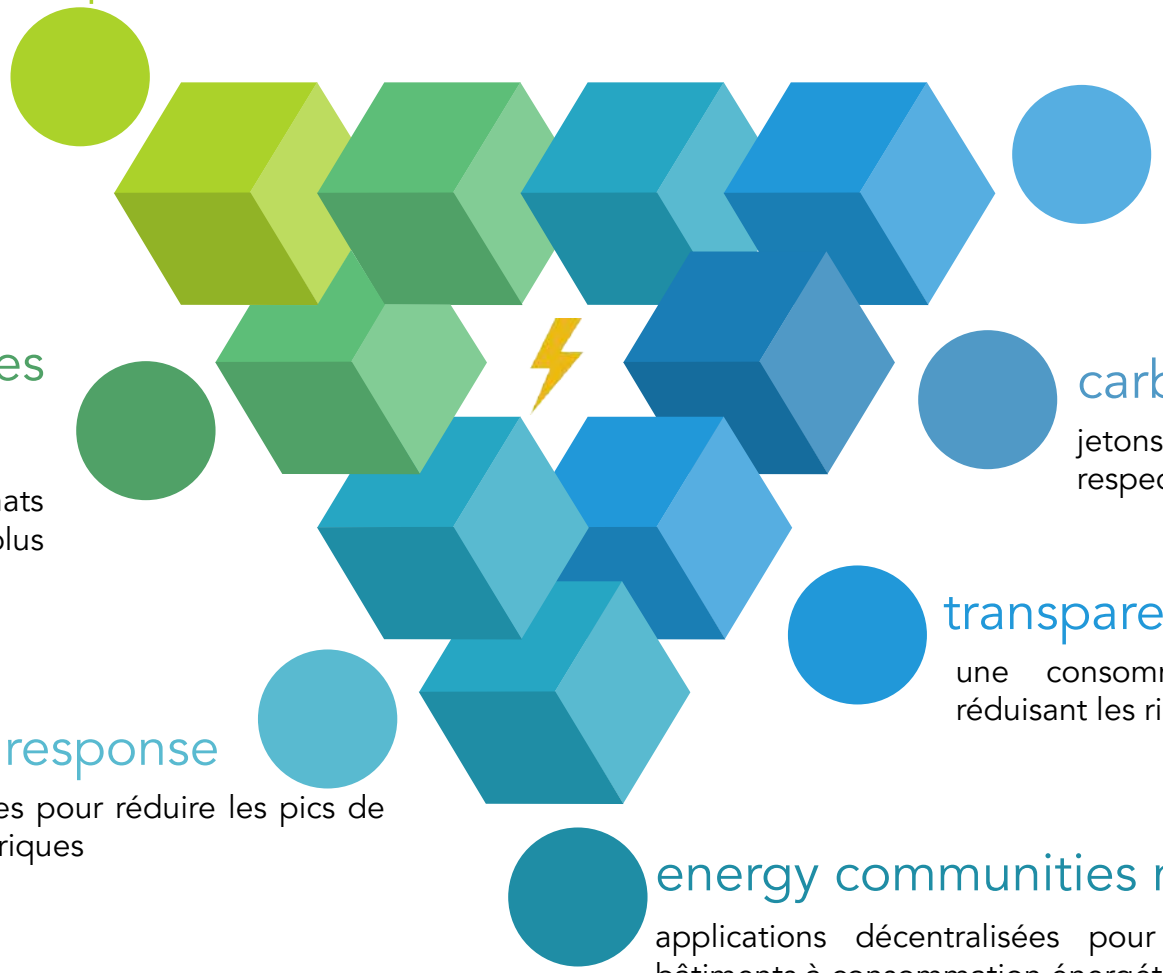


Blockchain

Opportunités d'utiliser la blockchain pour économiser de l'énergie

peer-to-peer energy marketplaces

personnes capables de vendre/acheter leur propre énergie



sectorial energy blockchain

une blockchain sectorielle interconnectée avec d'autres blockchains (finance, supply chain, etc.)

semi-connected devices use pay-as-you-go

économie mobile pour les micro-achats d'électricité dans les régions les plus pauvres du monde

carbon credits tracking

jetons utilisés comme mécanisme pour faire respecter les initiatives climatiques mondiales

transparent pricing/billing

une consommation suivie en toute transparence, réduisant les risques de fraude

manage demand-side response

orchestrer la demande des ménages pour réduire les pics de consommation sur les réseaux électriques

energy communities management

applications décentralisées pour gérer les communautés de bâtiments à consommation énergétique zéro

Blockchain

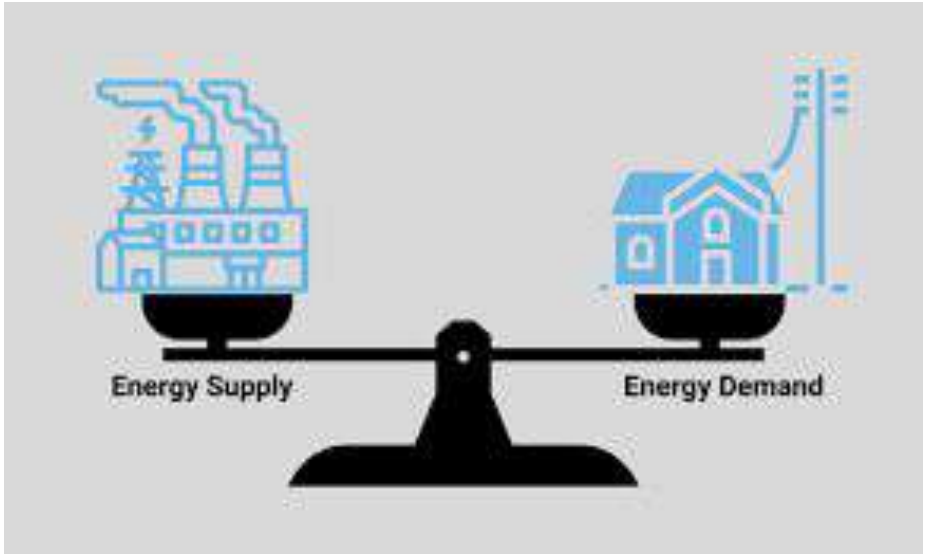
Opportunités d'utiliser la blockchain pour économiser de l'énergie

peer-to-peer energy marketplaces

personnes capables de vendre/acheter leur propre énergie

semi-connected devices use pay-as-you-go

économie mobile pour les micro-achats d'électricité dans les régions les plus pauvres du monde



manage demand-side response

orchestrer la demande des ménages pour réduire les pics de consommation sur les réseaux électriques

Blockchain

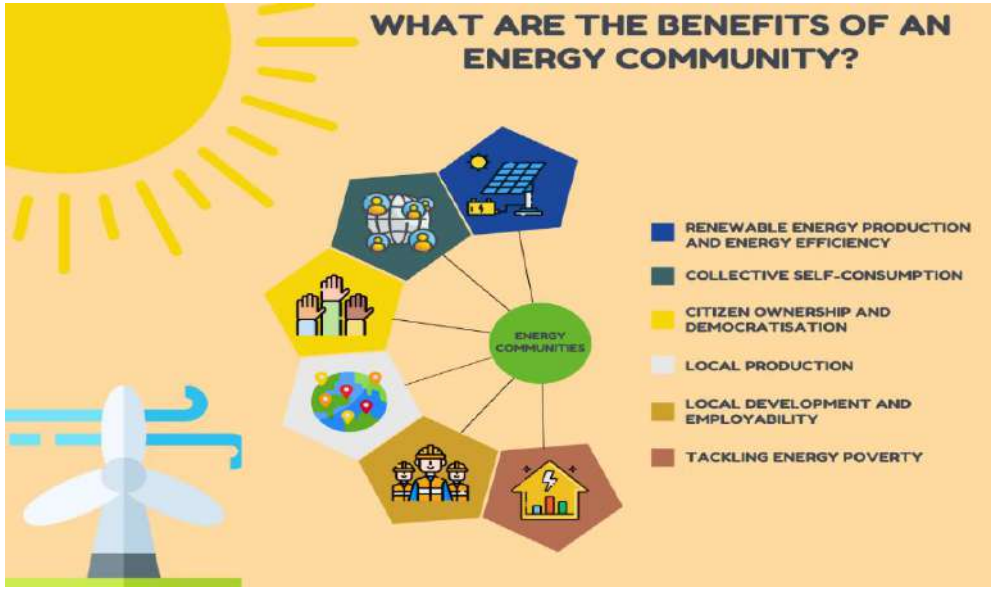
Opportunités d'utiliser la blockchain pour économiser de l'énergie

carbon credits tracking

jetons utilisés comme mécanisme pour faire respecter les initiatives climatiques mondiales

transparent pricing/billing

une consommation suivie en toute transparence, réduisant les risques de fraude



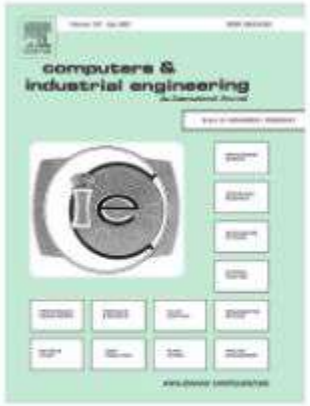
energy communities management

applications décentralisées pour gérer les communautés de bâtiments à consommation énergétique zéro

Journal

Journal

https://www.journals.elsevier.com/computers-and-industrial-engineering/call-for-papers/blockchain-based-applications



Special Issue Call for Papers: Blockchain-based applications for enhancing cybersecurity in manufacturing and building supply chain resilience - Call for Papers - Elsevier

CiteScore: 6.6 i CiteScore: 2020: 6.6 CiteScore measures the average citations received per peer-reviewed document published in this title. CiteScore values are based on citation counts in a range of four years (e.g. 2016-2019) to peer-reviewed documents (articles, reviews, conference papers, data papers and book chapters) published in the

www.journals.elsevier.com

End

Merci pour votre attention

Pour me contacter :

kzkik@esaip.org

Site web:

https://karimzkik.com
https://ma.linkedin.com/in/karim-zkik/

Vous pouvez me retrouver aussi sur :

DBLP, Google Scholar, ResearchGate, ORCID et Scopus

Vous êtes au ♡ du numérique !

www.adnouest.org

Partagez votre expérience : #JNR2022

@adnouest