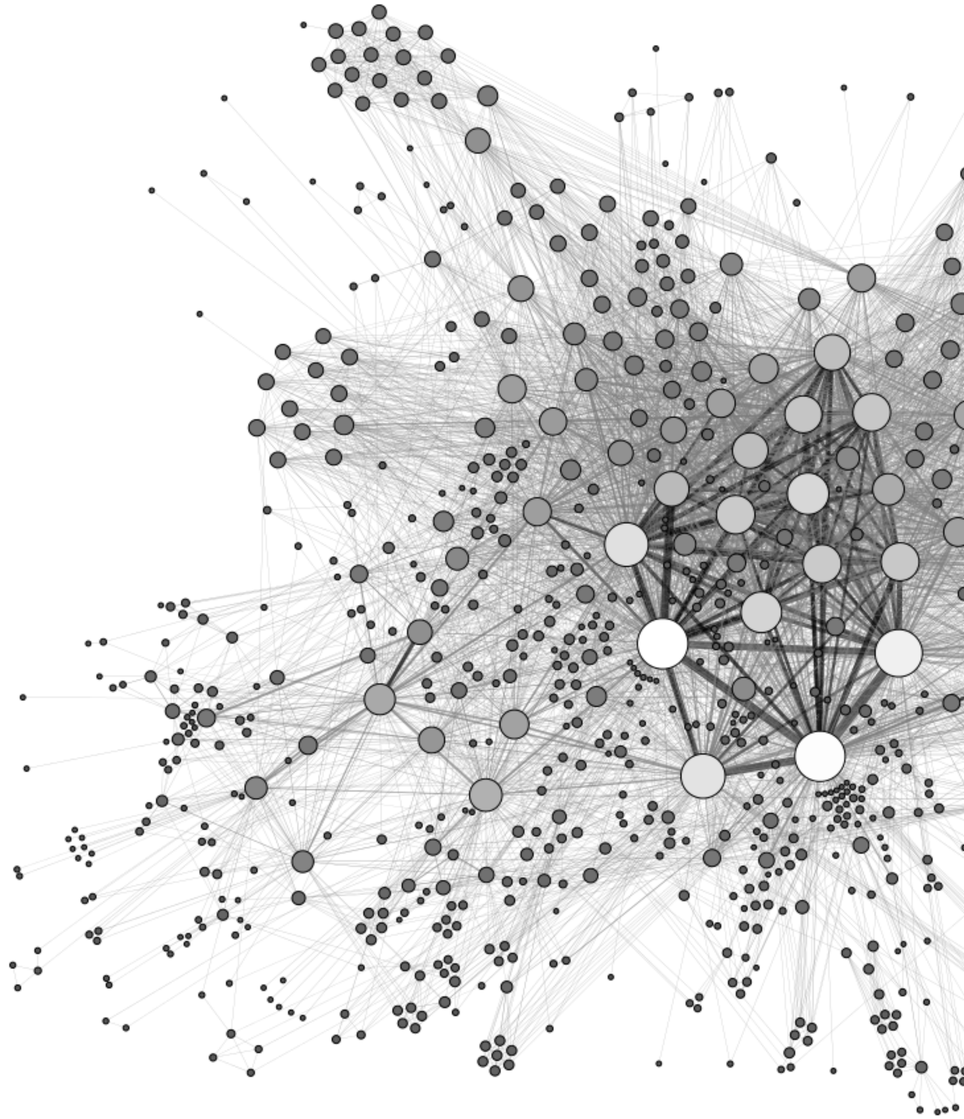
Bitcoin - Peut-on faire confiance ?

Coeur des Sciences - UQAM

Régis Barondeau, Ph.D.

Professeur substitut en management et technologie
ESG UQAM
barondeau.regis@uqam.ca
linkedin.com/in/regisbarondeau
www.regisbarondeau.com

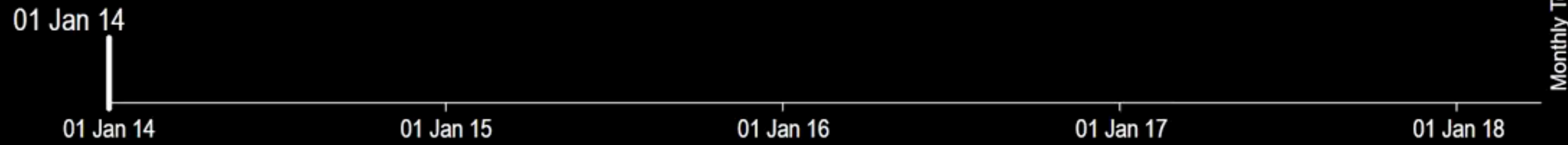
15 mai 2018



$0

Source : https://youtu.be/rIMKNkF6d28

Token Sales, 2014-Present



elementus

Qu’est-ce que le réseau Bitcoin ?

Photo par Thought Catalog on Unsplash


INSIDE THIS WEEK: TECHNOLOGY QUARTERLY
The Economist
The king's role in Thailand's chaos
Eurabian cities
After Mumbai
Sperm and intelligence
Our books of the year
Where have all your savings gone?


INSIDE: A 14-PAGE SPECIAL REPORT ON CARS IN EMERGING MARKETS
The Economist
Can China save the world?
In search of Republican brains
Life without nuclear weapons
The threat of deflation
Sarkozy, the secret socialist
Redesigning global finance
WTO
BRETTON WOODS
IMF

2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

2008

Précurseurs

- Signature numérique : clés publiques/privées (Diffie and Hellman, 1976)
- *The Byzantine Generals Problem*, (Lamport et al. 1982)
- Monnaie numérique (Chaum, 1983) -> DigiCash en 1994
- Horodatage (Haber et al.,1990)
- Peer to peer (P2P) fin 90 -> Napster
- *Hashcash* (Back, 2002)
- …

Innovation

- Combinaison de technologies existantes
- Invention du *consensus de Nakamoto*

Le *consensus de Nakamoto* est un mécanisme de compétition en ligne qui consiste à résoudre un problème mathématique.

Celui-ci demande un investissement énergétique qui crée un équilibre dans le réseau.

Qu’est-ce qu’un bitcoin ?

Une monnaie numérique pour l’Internet que l’on peut dépenser, transférer ou stocker.

Un progrès dans l’histoire de la monnaie

Photo par Baomi

Photo par Elaine Robin

Photo by Ján Jakub Naništa on Unsplash

Photo par cgb

Photo par Lotus Head

La monnaie n’est-elle pas déjà numérique ?

Messari, 1340

Résumé - Bitcoin

- Premier réseau blockchain
- Première monnaie numérique (fonctionnelle)
- Monnaie indépendante du système bancaire
- Premier actif numérique rare (≠ double-spending)
- Suppression de la comptabilité en partie double
- Suppression des intermédiaires
- Consensus par le code => confiance
- Registre distribué => décentralisation

Source : https://icons8.com/icon/new-icons/all

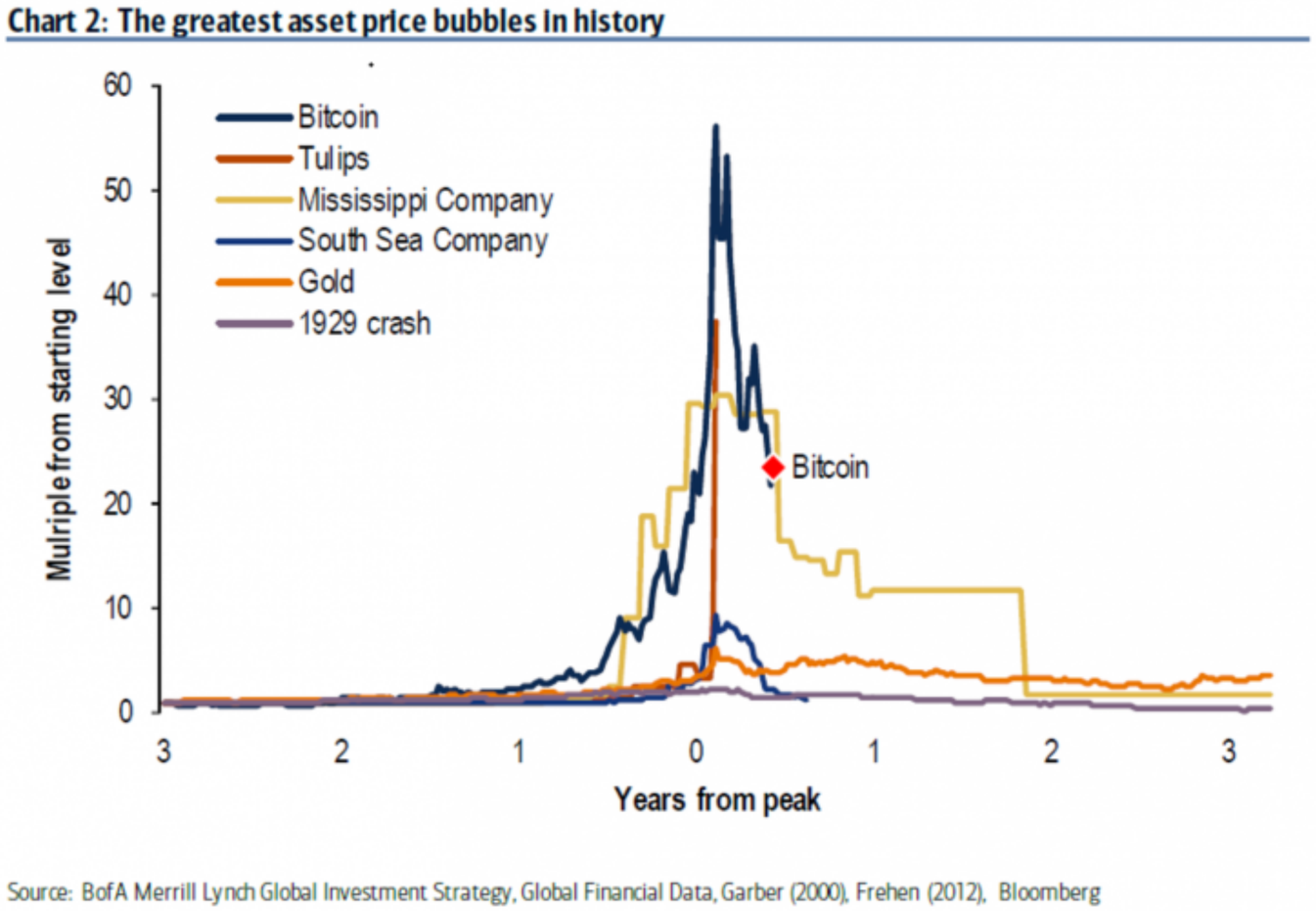
Faut-il acheter des bitcoins ?

« Bitcoin is rat poison squared. »

« You don’t really have anything that has produced anything.
You’re just hoping the next guy pays more. »

Warren Buffett, 7 mai 2018

Bank of America: Bitcoin Bubble Is Already Popping



Source : https://www.bloomberg.com/news/articles/2018-05-05/white-house-blasts-china-for-its-censorship-of-u-s-airlines

Photo by Kristina Bratko on Unsplash

- Rareté
- Adoption large
- Précurseur
- Sous-évaluation
- Règlementation favorable
- Diversification du portefeuille

- Échec de la transition en 2040
- Problème de gouvernance
- Protocole concurrent
- Volatilité
- Règlementation défavorable
- Attaque du réseau

Source : https://icons8.com/icon/new-icons/all

Qu’est qu’un réseau blockchain ?

C’est un artefact crée par un mécanisme de consensus.

Plus précisément, c’est un registre distribué « infalsifiable » qui archive toutes les transactions depuis le début du réseau.

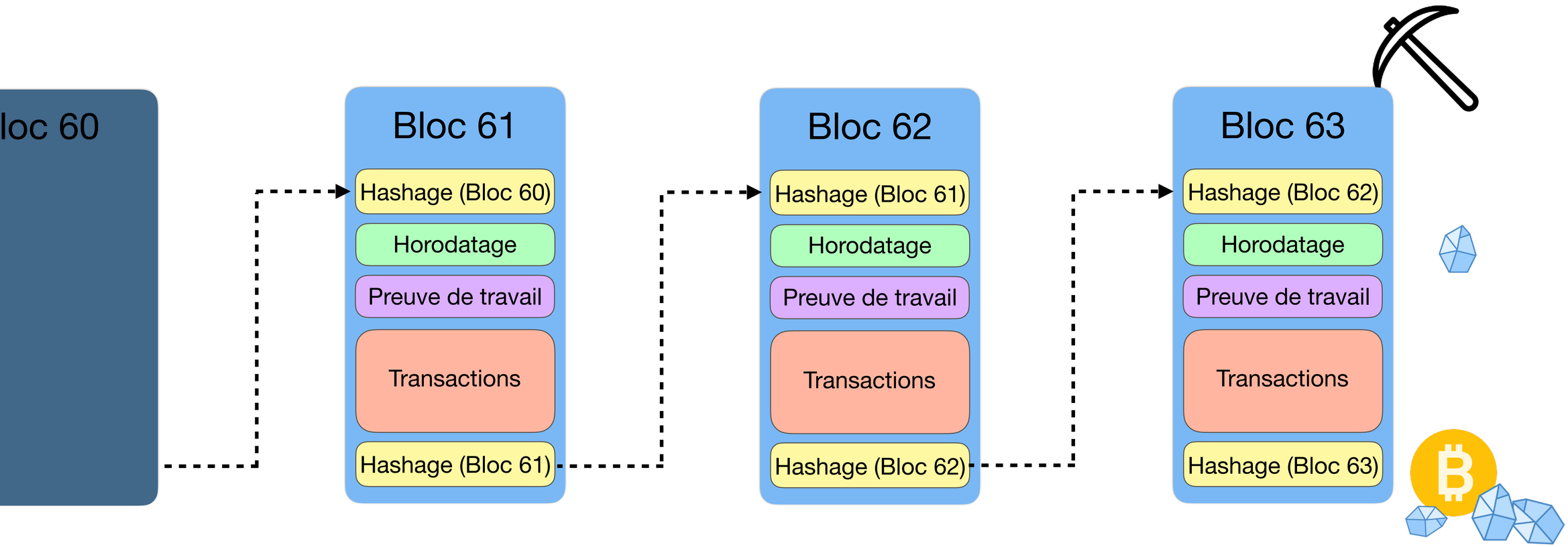
BITCOIN has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the "dark net".

This is unfair. The value of a bitcoin has been pretty stable, at around $250, for most of this year. Among regulators and financial institutions, scepticism has given way to enthusiasm (the European Union recently recognised it as a currency). But most unfair of all is that **bitcoin's shady image causes people to overlook the extraordinary potential of the "blockchain", the technology that underpins it.** This innovation carries a significance stretching far beyond cryptocurrency. The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. **Simply put, it is a machine for creating trust.**

Oct 31st 2015 | From the print edition

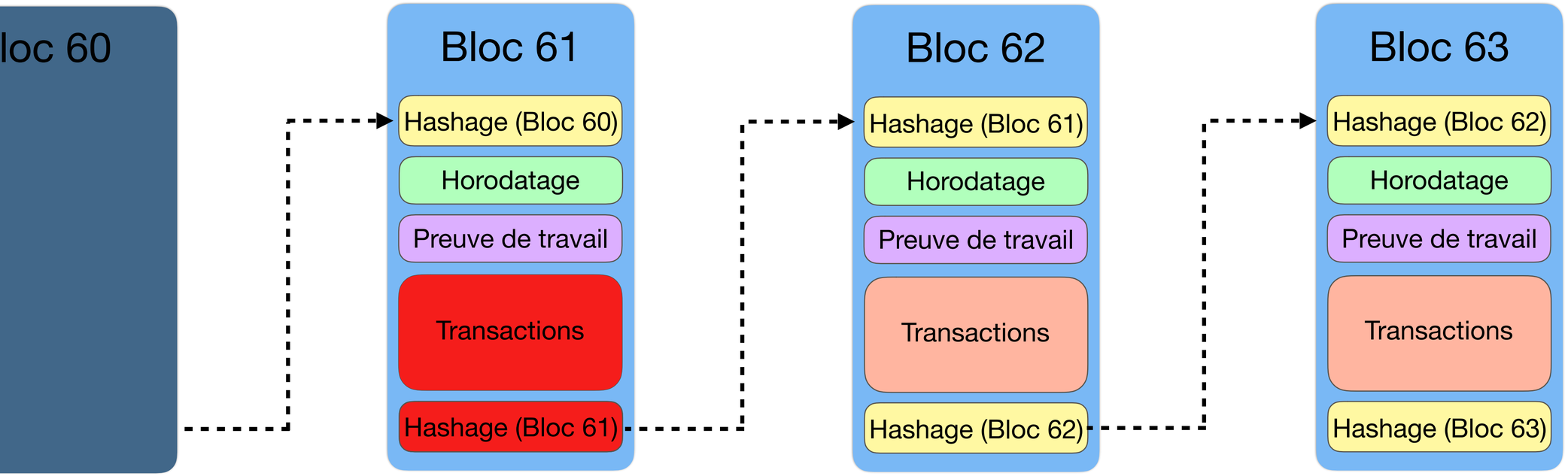
2015

Vue simplifiée du réseau blockchain Bitcoin

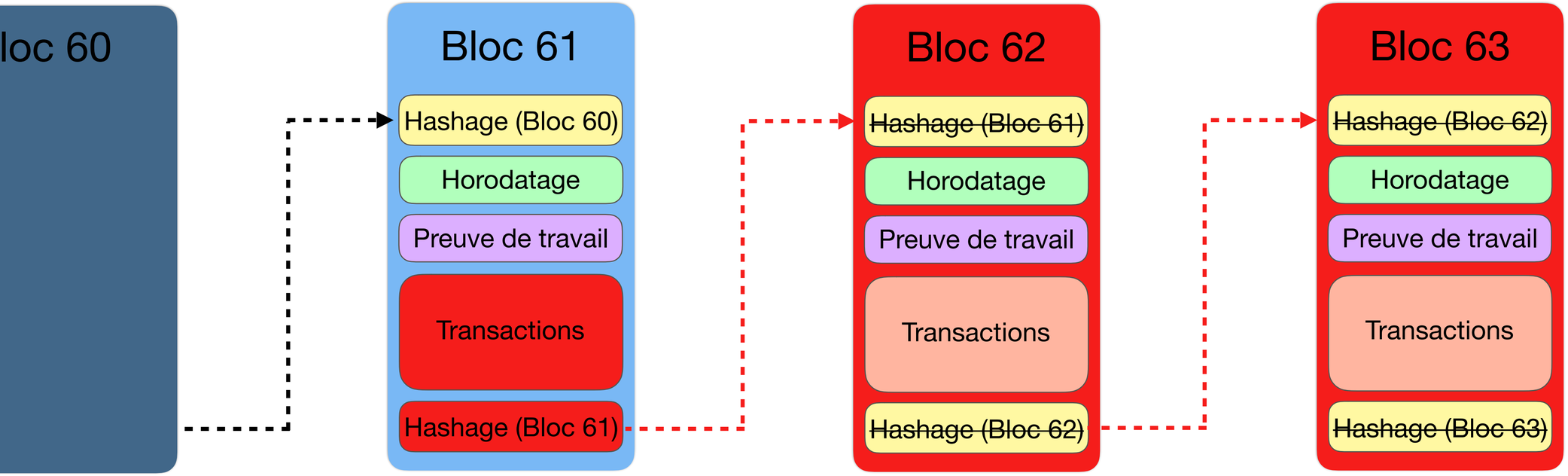


Miner = sécuriser le réseau

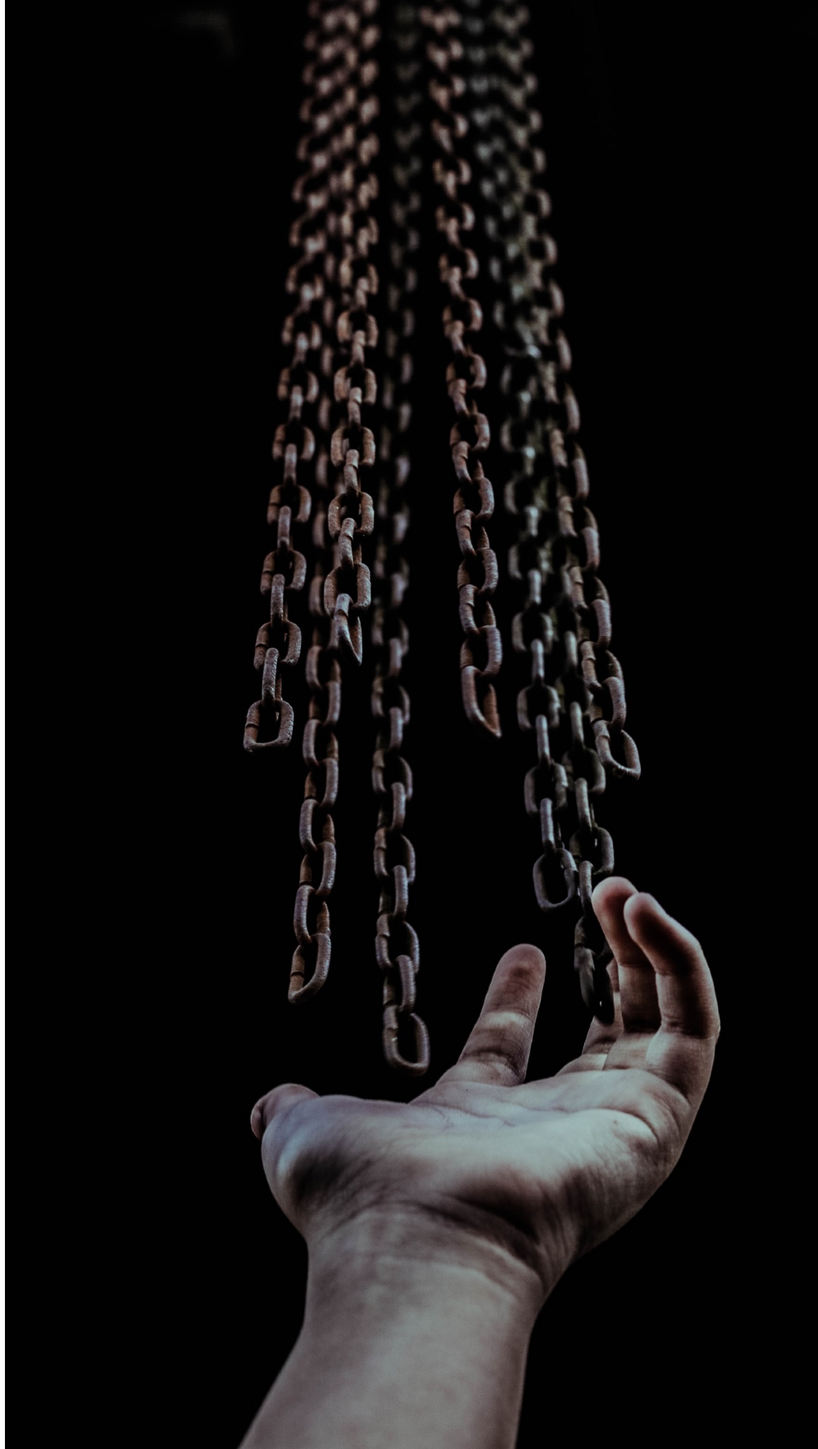
Vue simplifiée d’une tentative de corruption du réseau Bitcoin



Vue simplifiée d’une tentative de corruption du réseau Bitcoin



Il n’y a pas une blockchain mais des milliers de réseaux blockchain.

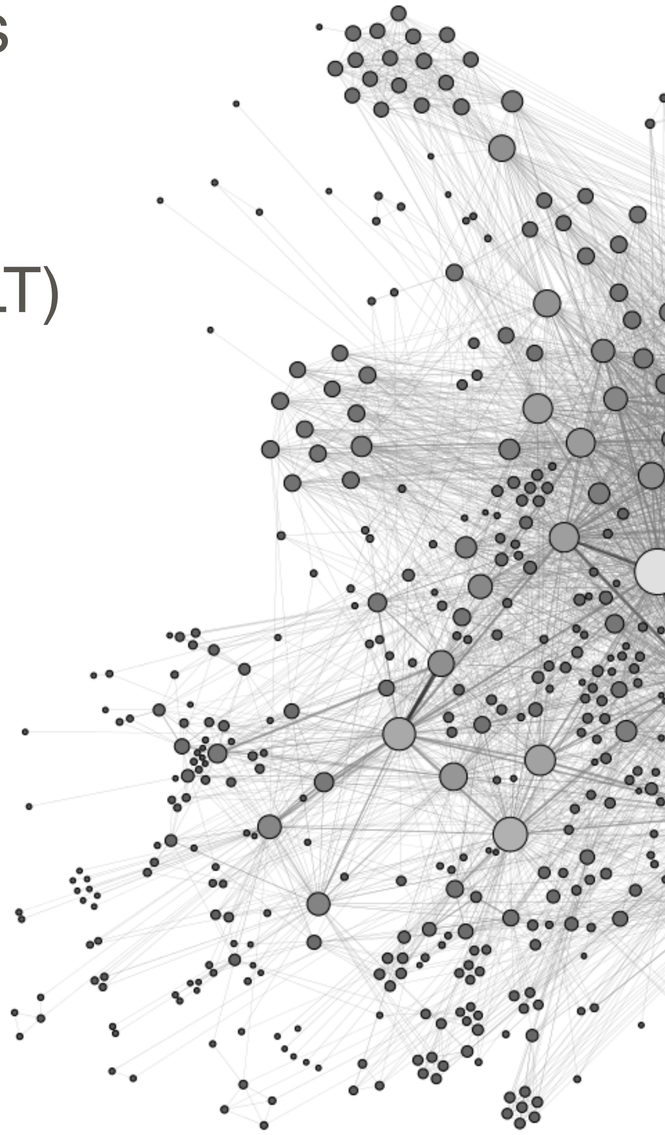


Source : Photo by Zulmaury Saavedra on Unsplash

Bitcoin : composantes et caractéristiques

- Un registre décentralisé (distributed ledger technology - DLT)
- Un actif cryptographique (token) -> incitatif
- Une signature numérique
- Un mécanisme de consensus

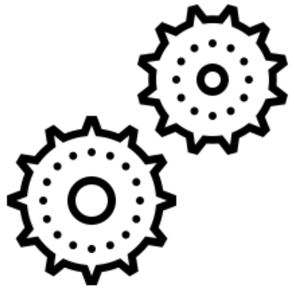
- Inviolable « en théorie » (tamper-proof)
- Irréversible
- Transparent
- Usage de pseudonymes (pseudonymity)



Une couche de confiance pour l’Internet

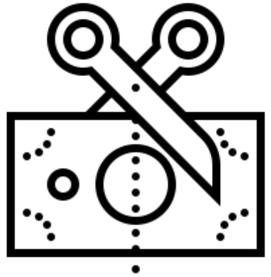
Source : https://icons8.com/icon/new-icons/all

Quels sont les risques associés aux actifs cryptographiques ?



Technologie

- Infrastructures
- Marchés
- Portefeuilles
- Fraudes

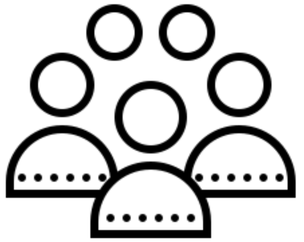


Fiscalité

- Utilisateurs
- Mineurs

Règlementation

- Marchés
- Types d’actifs
- Fongibilité



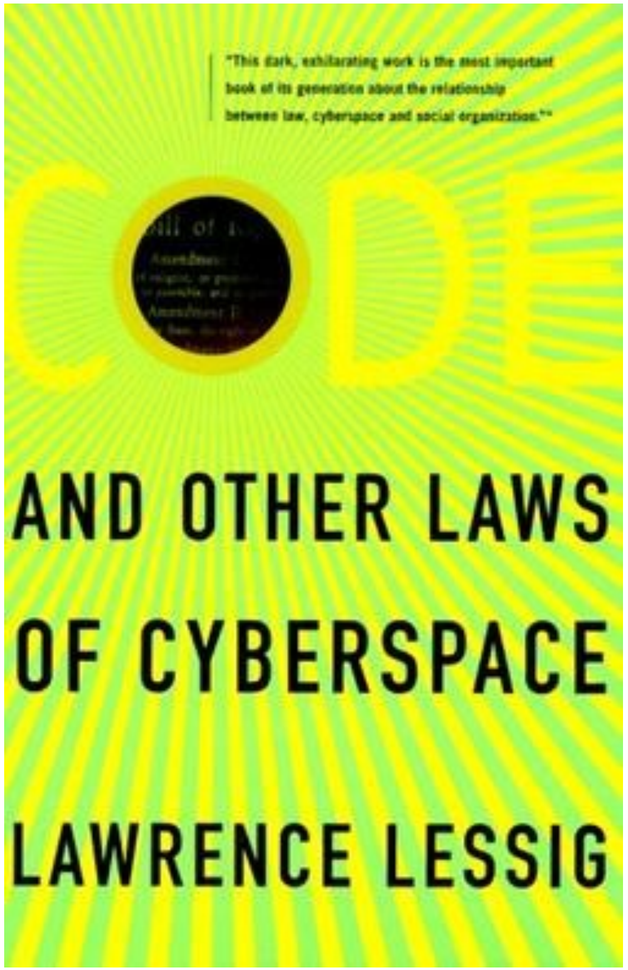
Adoption

- Projets pilotes
- Usages réels

Source : https://icons8.com/icon/new-icons/all

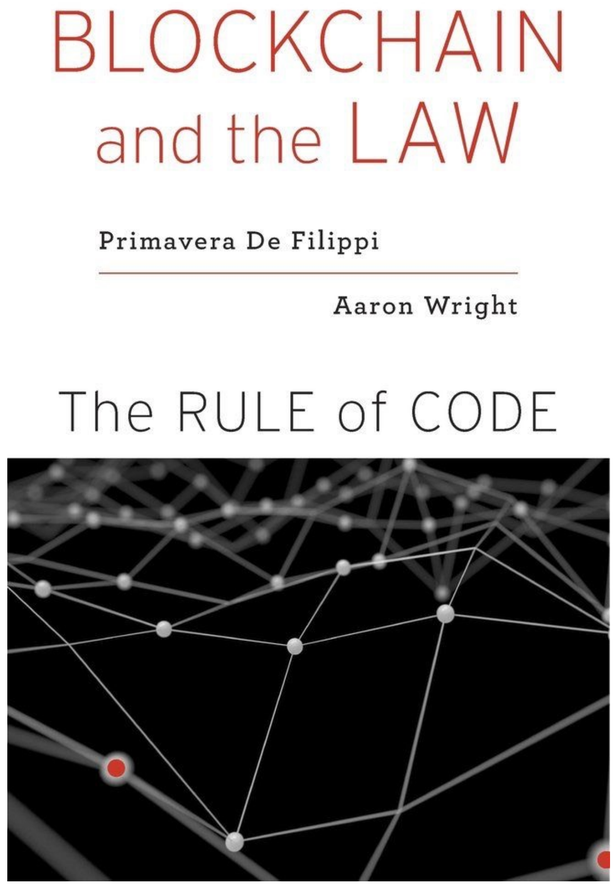
« Code is law. »

(Lessig, 2000)



Lex cryptographica

(De Filippi et Wright, 2018)

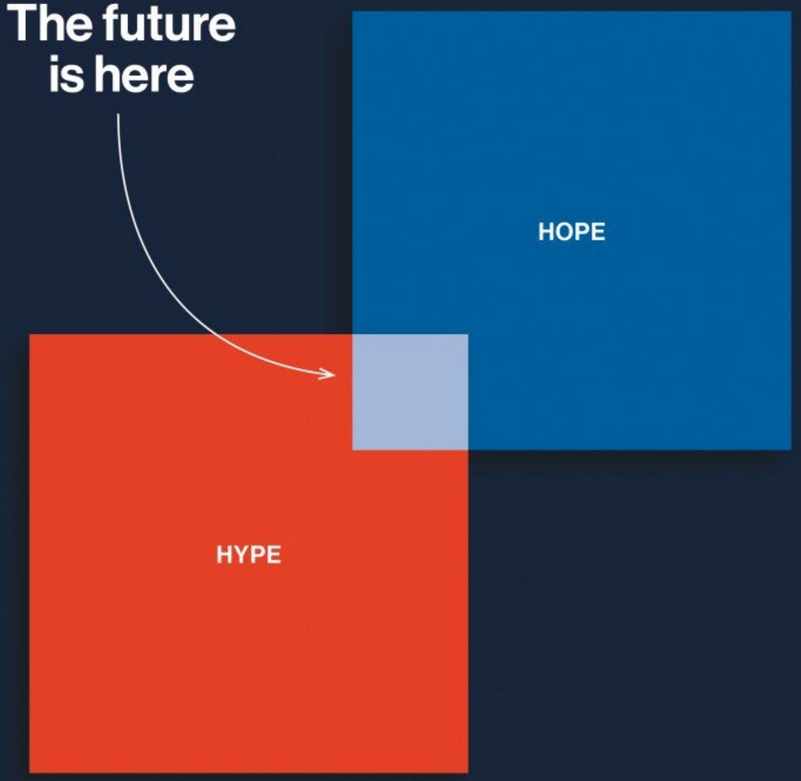


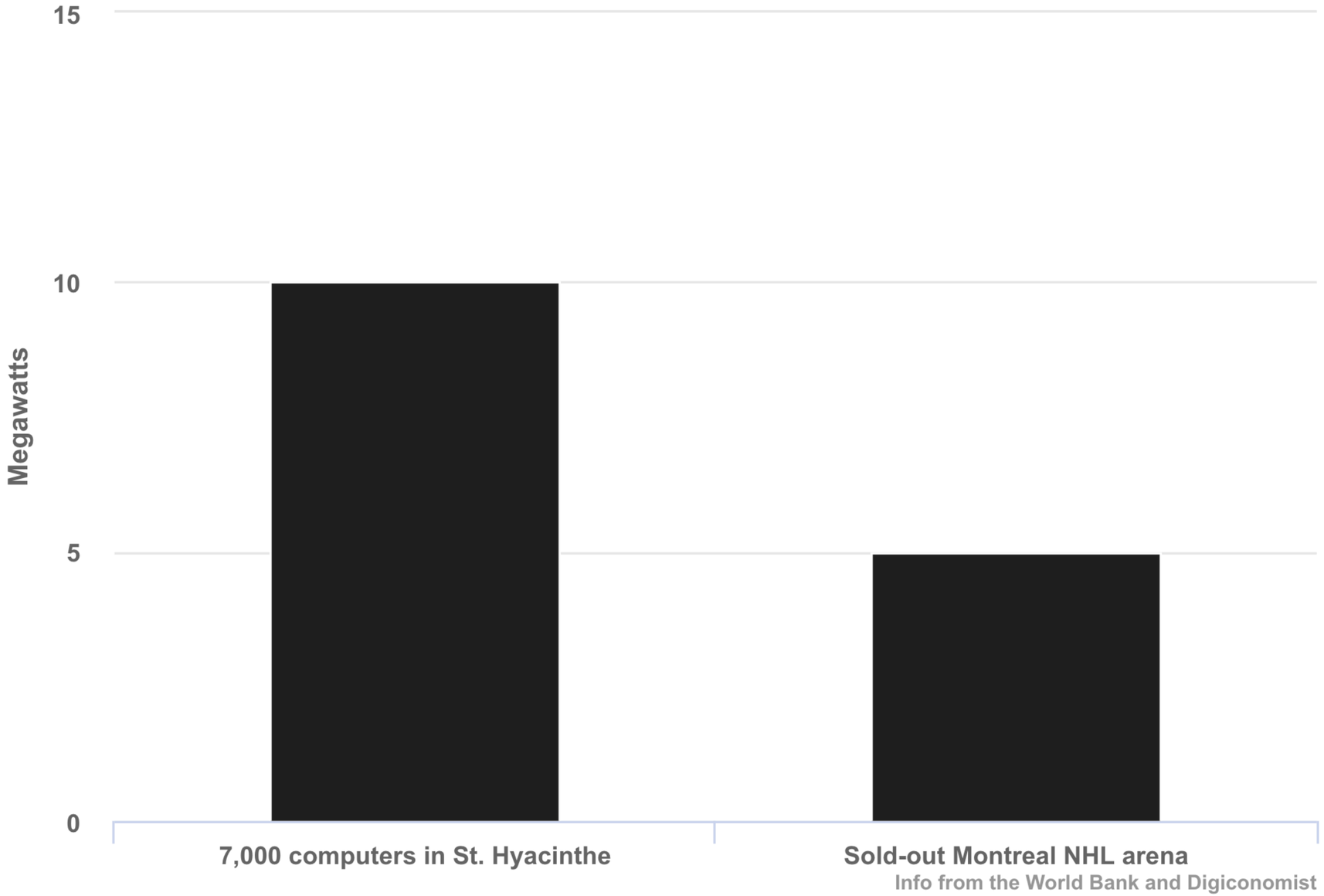
Quel est le coût énergétique des cryptomonnaies ?

MIT Technology Review

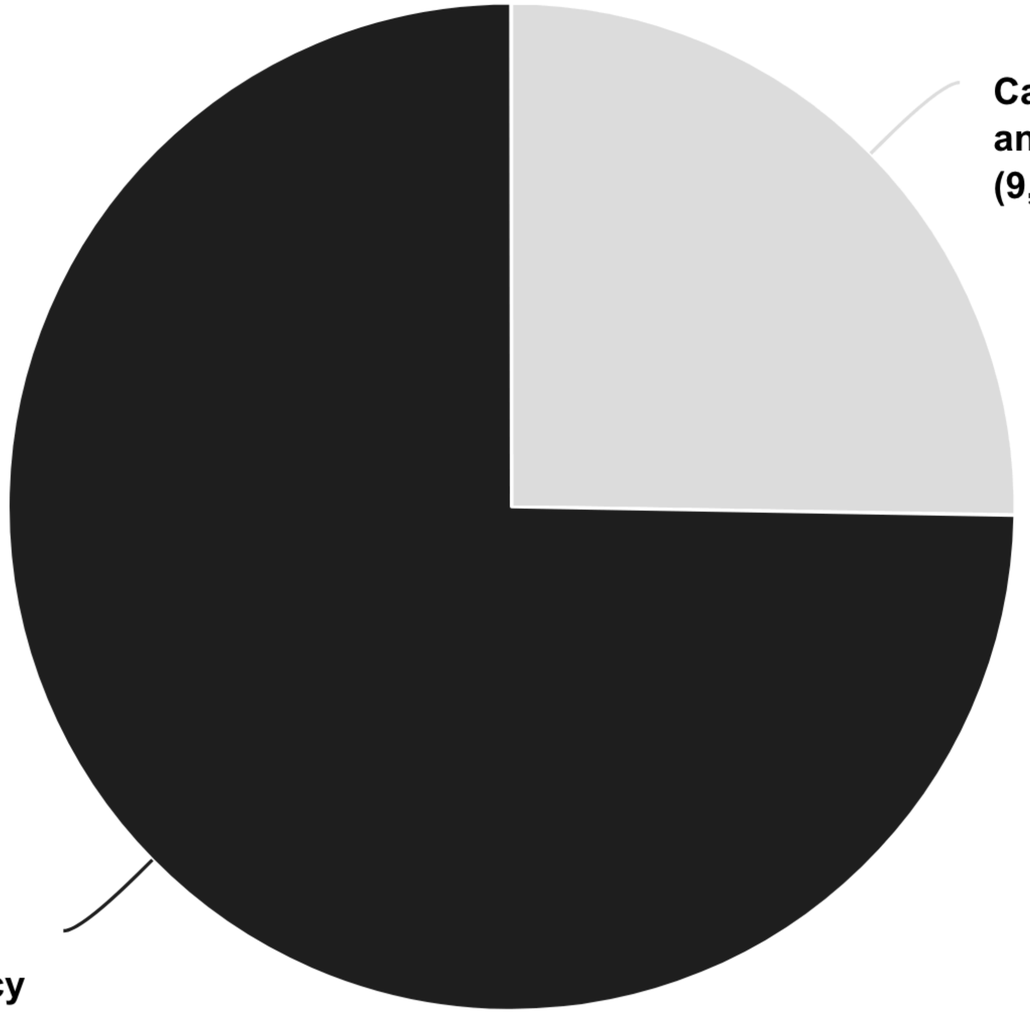
VOL. 121 NO. 3 MAY/JUNE 2018 US $6.99/CAN $7.99

Blockchain





Source : https://www.technologyreview.com/s/610786/bitcoin-is-eating-quebec/



Info from the World Bank and Digiconomist. Afghanistan figure is from 2014.

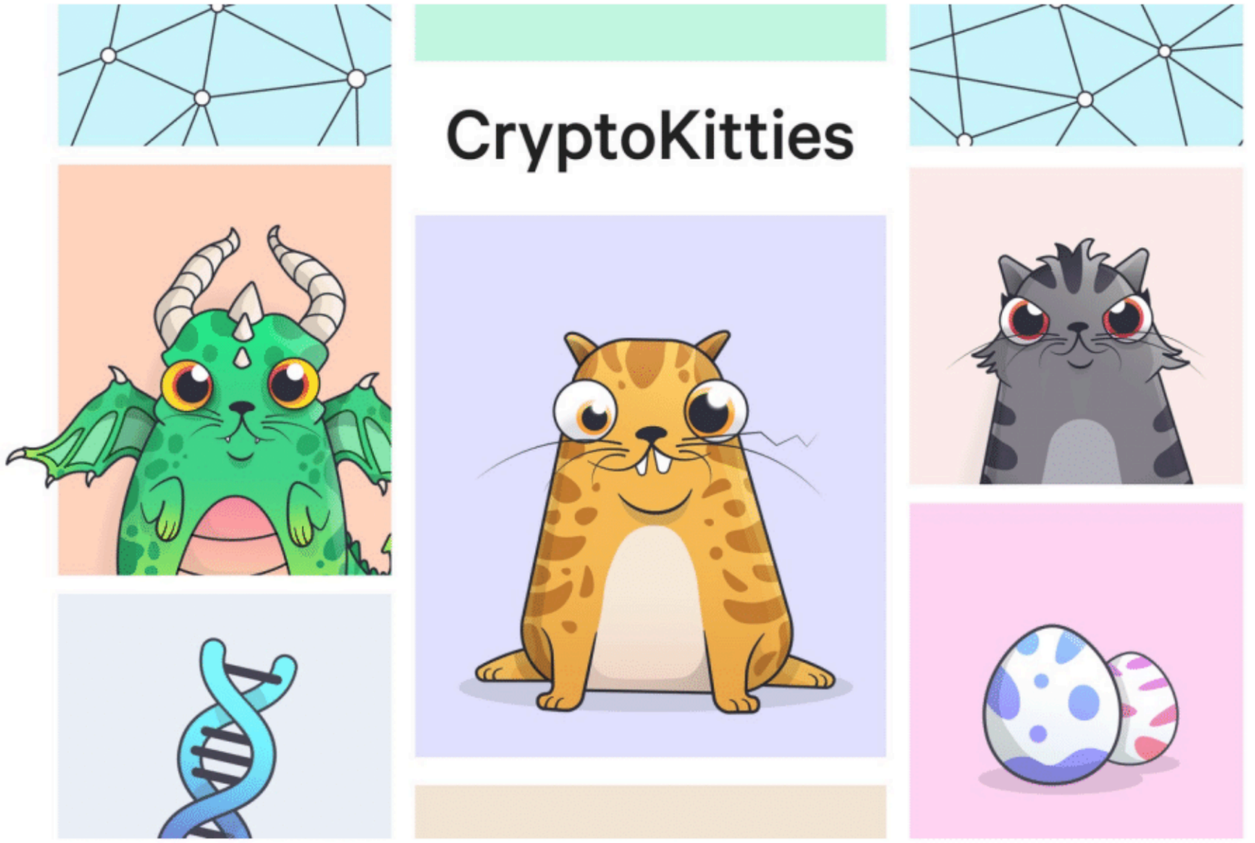
Source : https://www.technologyreview.com/s/610786/bitcoin-is-eating-quebec/

Qu’est-ce qu’Ethereum ?


ethereum
2014

Une monnaie programmable pour supprimer les intermédiaires à l’aide de contrats intelligents (smart contracts).

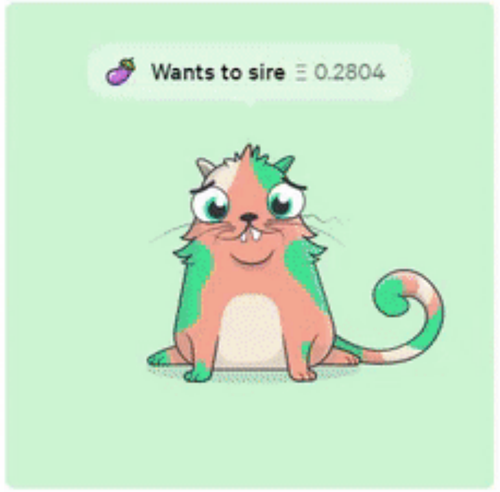
Paiement de machine à machine.



CryptoKitties: Collectible and Breedable Cats Empowered by Blockchain Technology

WHITE PA-PURR

Source : https://www.cryptokitties.co/



Kitty #72418

Kitty #72418 · Gen 4

Swift

Virgin Snappy G8

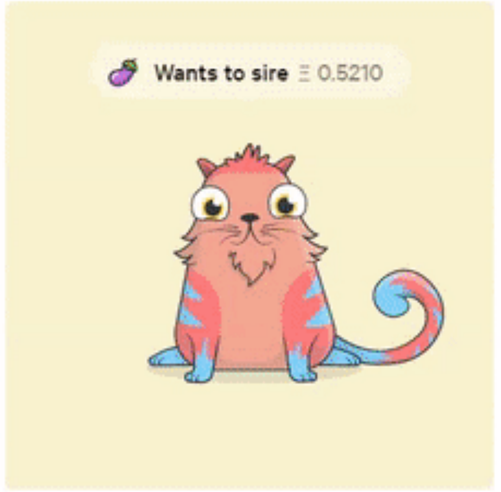
Kitty #72332 · Gen 8

Snappy

Kitty #71954

Kitty #71954 · Gen 15

Plodding



GoldSkyblue Tigerpunk

Kitty #71941 · Gen 15

Plodding

Source : https://github.com/HaJaeKyung/KittyExtension

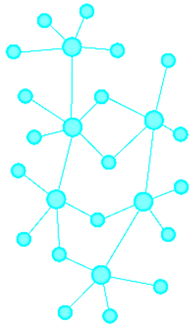
DAO

Decentralized Autonomous Organization

The DAO

Pourquoi utiliser l’innovation blockchain ?

Coûts de transaction
(Coase, 1938)

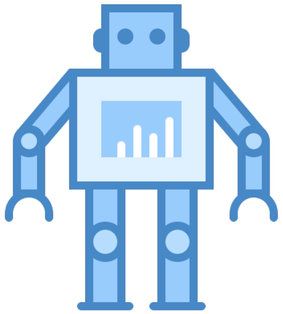


Décentralisation

Sécurité

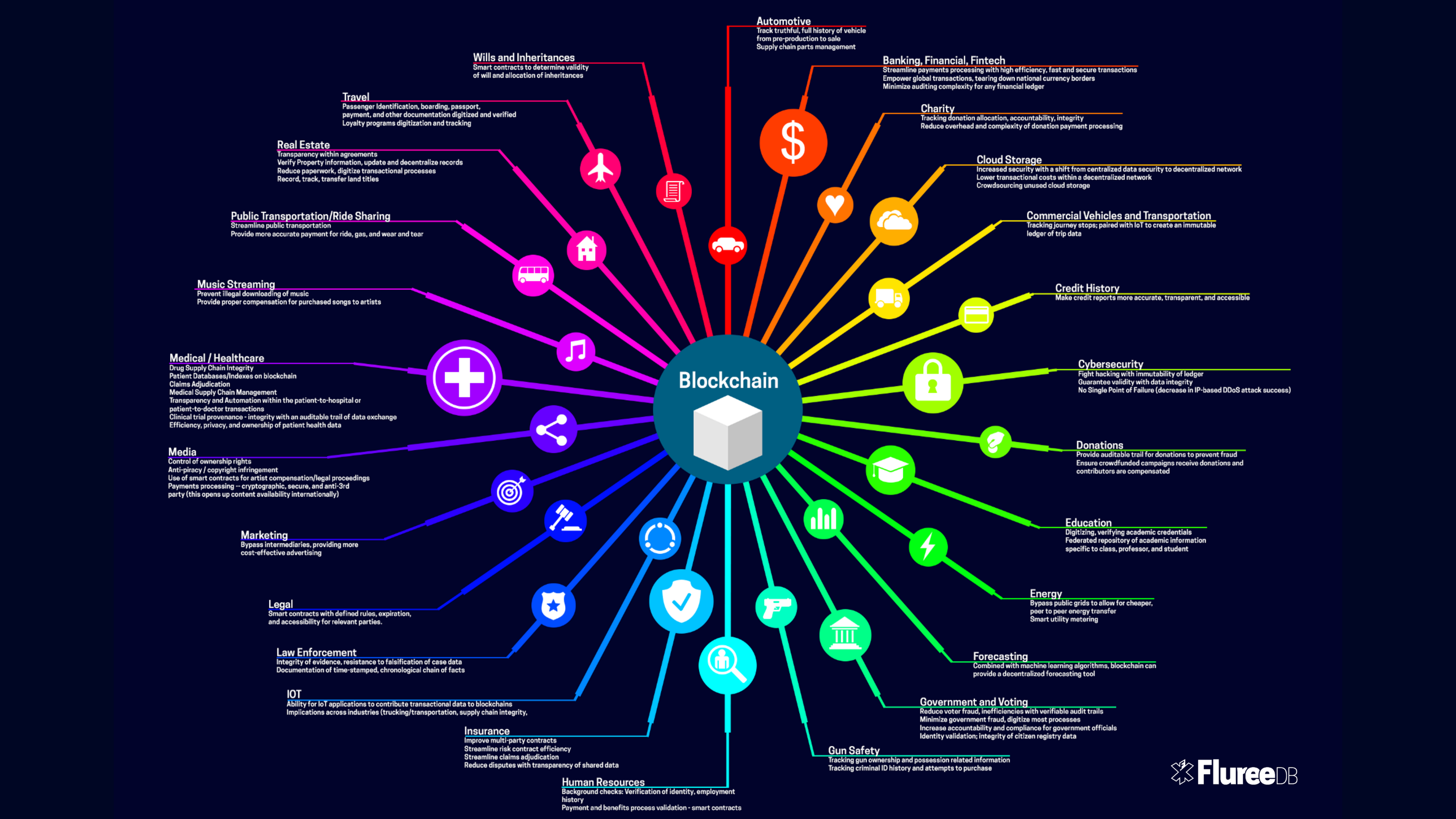
Performance

Audit

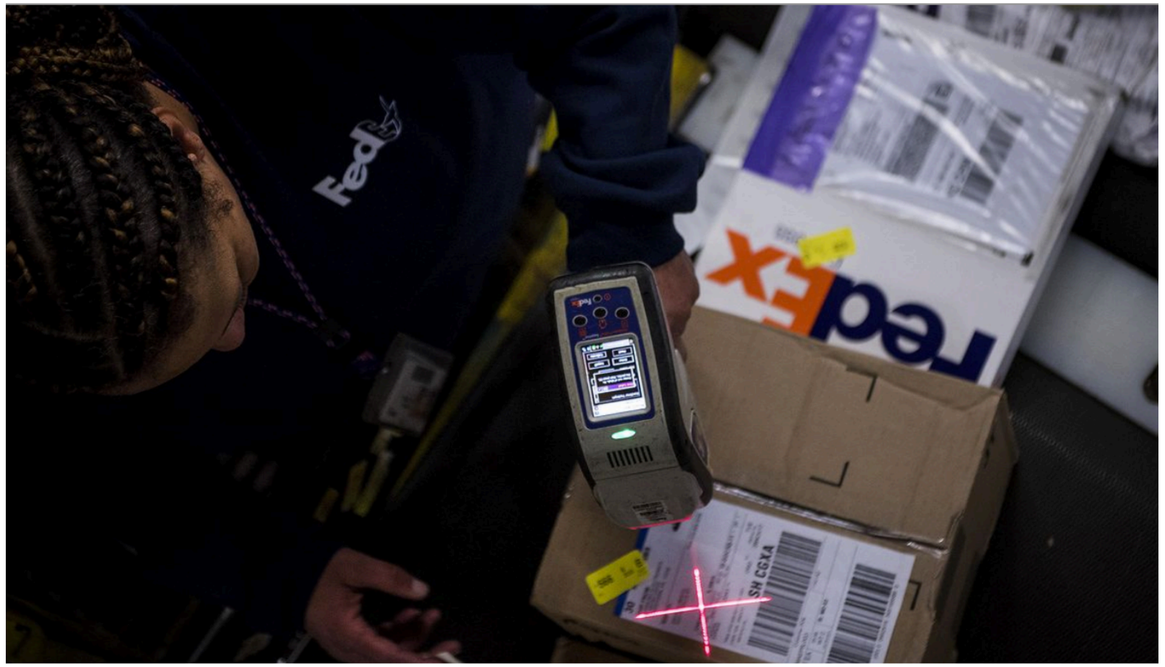


Automatisation

Source : https://icons8.com/icon/new-icons/all


Blockchain
Automotive
Track truthful, full history of vehicle from pre-production to sale
Supply chain parts management
Banking, Financial, Fintech
Streamline payments processing with high efficiency, fast and secure transactions
Empower global transactions, tearing down national currency borders
Minimize auditing complexity for any financial ledger
Charity
Tracking donation allocation, accountability, integrity
Reduce overhead and complexity of donation payment processing
Cloud Storage
Increased security with a shift from centralized data security to decentralized network
Lower transactional costs within a decentralized network
Crowdsourcing unused cloud storage
Commercial Vehicles and Transportation
Tracking journey stops; paired with IoT to create an immutable ledger of trip data
Credit History
Make credit reports more accurate, transparent, and accessible
Cybersecurity
Fight hacking with immutability of ledger
Guarantee validity with data integrity
No Single Point of Failure (decrease in IP-based DDoS attack success)
Donations
Provide auditable trail for donations to prevent fraud
Ensure crowdfunded campaigns receive donations and contributors are compensated
Education
Digitizing, verifying academic credentials
Federated repository of academic information specific to class, professor, and student
Energy
Bypass public grids to allow for cheaper, peer to peer energy transfer
Smart utility metering
Forecasting
Combined with machine learning algorithms, blockchain can provide a decentralized forecasting tool
Government and Voting
Reduce voter fraud, inefficiencies with verifiable audit trails
Minimize government fraud, digitize most processes
Increase accountability and compliance for government officials
Identity validation; integrity of citizen registry data
Gun Safety
Tracking gun ownership and possession related information
Tracking criminal ID history and attempts to purchase
Human Resources
Background checks: Verification of identity, employment history
Payment and benefits process validation - smart contracts
Insurance
Improve multi-party contracts
Streamline risk contract efficiency
Streamline claims adjudication
Reduce disputes with transparency of shared data
IOT
Ability for IoT applications to contribute transactional data to blockchains
Implications across industries (trucking/transportation, supply chain integrity,
Law Enforcement
Integrity of evidence, resistance to falsification of case data
Documentation of time-stamped, chronological chain of facts
Legal
Smart contracts with defined rules, expiration, and accessibility for relevant parties.
Marketing
Bypass intermediaries, providing more cost-effective advertising
Media
Control of ownership rights
Anti-piracy / copyright infringement
Use of smart contracts for artist compensation/legal proceedings
Payments processing -- cryptographic, secure, and anti-3rd party (this opens up content availability internationally)
Medical / Healthcare
Drug Supply Chain Integrity
Patient Databases/Indexes on blockchain
Claims Adjudication
Medical Supply Chain Management
Transparency and Automation within the patient-to-hospital or patient-to-doctor transactions
Clinical trial provenance - integrity with an auditable trail of data exchange
Efficiency, privacy, and ownership of patient health data
Music Streaming
Prevent illegal downloading of music
Provide proper compensation for purchased songs to artists
Public Transportation/Ride Sharing
Streamline public transportation
Provide more accurate payment for ride, gas, and wear and tear
Real Estate
Transparency within agreements
Verify Property information, update and decentralize records
Reduce paperwork, digitize transactional processes
Record, track, transfer land titles
Travel
Passenger Identification, boarding, passport, payment, and other documentation digitized and verified
Loyalty programs digitization and tracking
Wills and Inheritances
Smart contracts to determine validity of will and allocation of inheritances
FlureeDB

Bloomberg



Photographer: Christopher Dilts/Bloomberg

Cryptocurrencies

FedEx's Smith Sees Blockchain as `Next Frontier' for Logistics

By Thomas Black
14 mai 2018 à 12:22 UTC−4

“It’s the next frontier that’s going to completely change worldwide supply chains.”

Fred Smith, CEO Fedex, 14 mai 2018

Source :https://www.bloomberg.com/news/articles/2018-05-14/fedex-s-smith-sees-blockchain-as-next-frontier-for-logistics

« Si la technologie blockchain mûrit, nous devrons peut-être nous demander si nous préférons vivre dans un monde où la plupart de nos transactions économiques et de nos interactions sociales sont régulées par les règles de droit — qui sont universelles, mais aussi plus souples et ambiguës, et donc pas toujours clairement applicables — ou si nous préférons nous soumettre aux règles du code. Les applications décentralisées basées sur les réseaux blockchains nous libèrent peut-être de la tyrannie de centralisation des intermédiaires et des tiers de confiance, mais cette libération pourrait se faire au prix d'une menace beaucoup plus grande — celle de tomber sous le joug de la tyrannie du code. »

[Notre traduction] (De Filippi et Wright, 2018 p. 210)

On sur-estime les technologies à court-terme
et on les sous-estime à long-terme.

Merci!

Régis Barondeau, Ph.D.

Professeur substitut en management et technologie
ESG UQAM
barondeau.regis@uqam.ca
linkedin.com/in/regisbarondeau
www.regisbarondeau.com