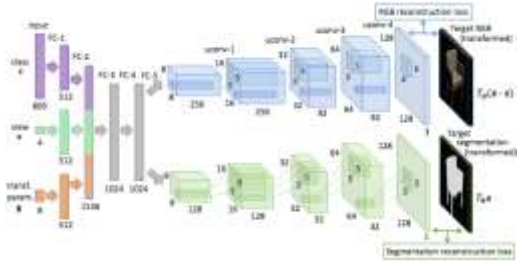
prospective numérique
et régulation des télécoms

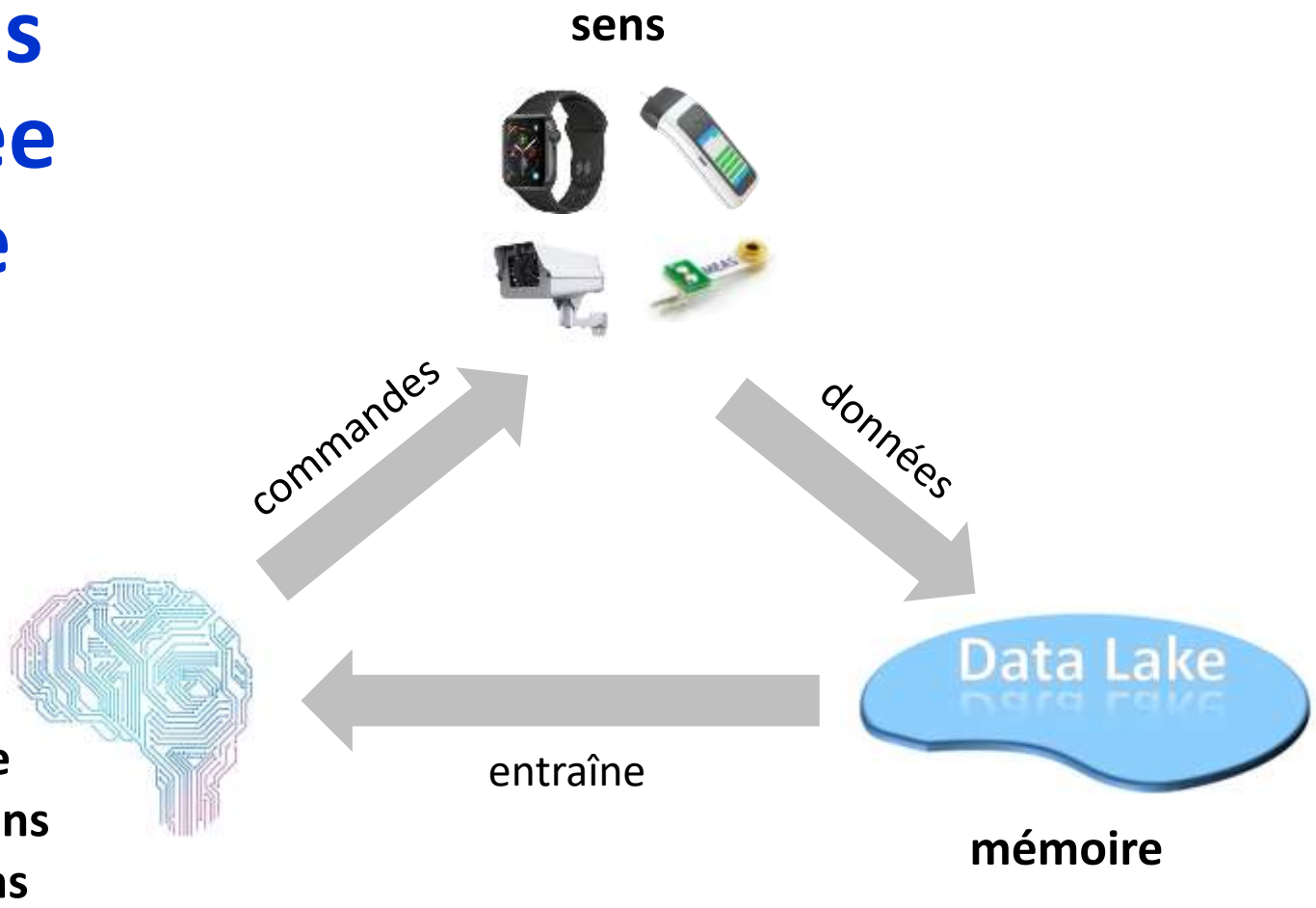
olivier ezratty
consultant et auteur
olivier@oezratty.net **www.oezratty.net** **@olivez**

FRATEL, Paris, 23 novembre 2018



BLOCKCHAIN

télécoms
vie privée
énergie



tsunami *à terme* des véhicules autonomes

"car as a service"

assurances

moins de voitures

immobilier

plateformisation

travail et loisirs

gestion du temps

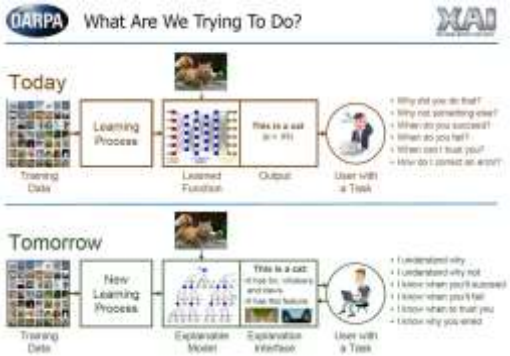
énergies renouvelables

smart city

personnalisation numérique

quelques enjeux de l'IA

données



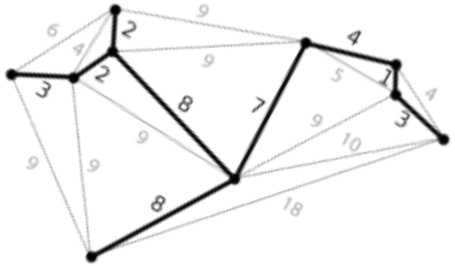
explicabilité

processeurs

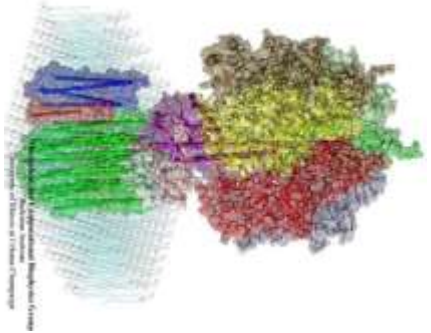
vie privée

télémédecine

applications du calcul quantique

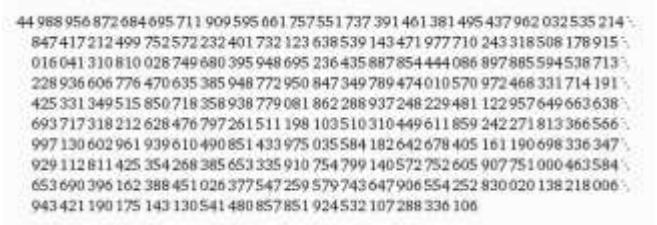


optimisations combinatoires
trajets, placements, cartes, finance



simulations moléculaires
matériaux et biologie

intelligence artificielle
machine learning et deep learning



factorisation
de très grands nombres entiers

protocoles menacés

RSA, ECDH, ECDSA, SSH, TLS, IPSEC, PGP, Signal (Whatsapp)

non menacés

SHA-3, AES-256

MIT Technology Review

Business Impact

Quantum Computers Pose Imminent Threat to Bitcoin Security

The massive calculating power of quantum computers will be able to break Bitcoin security within 10 years, say security experts.

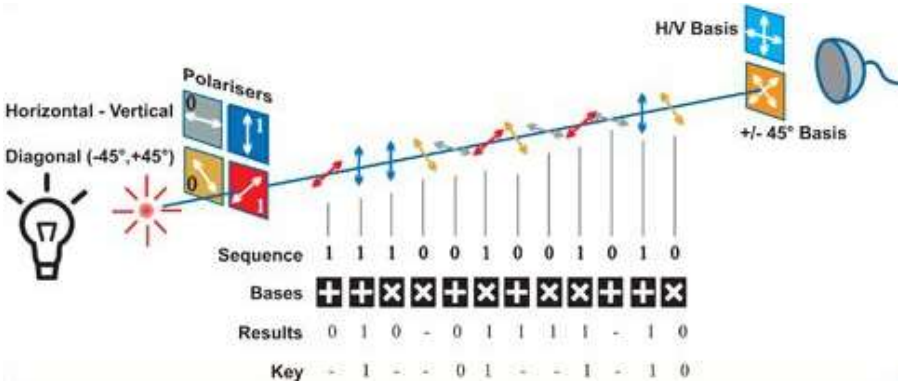
by Emerging Technology from the arXiv November 8, 2017

The Quantum Countdown
Quantum Computing And The Future Of Smart Ledger Encryption

Table 4. Risks to Blockchain Architectures from Quantum Computing

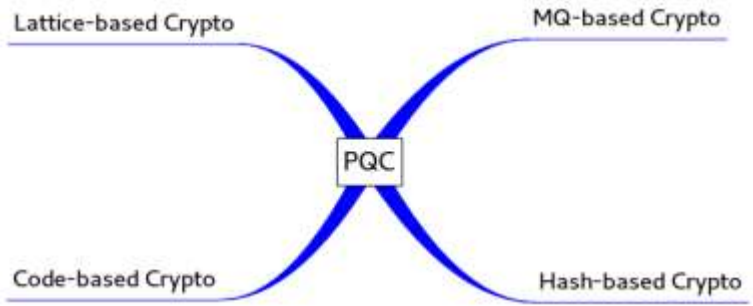
	Transactions	Data on Blockchain	Software on Blockchain
Read historical records without authorization	No (blockchains are intended to allow access to transaction information)	No, unless confidential and secured with vulnerable cryptography	No, unless confidential and secured with vulnerable cryptography
Alter historical records	No	No	May be able to run software without authorisation if signature used
Spoof ongoing records	Yes, possibly	Yes, possibly	Yes, possibly

clés quantiques QKD / BB84
protège les clés symétriques
par liaison optique



nouvelles infrastructures

chiffrements post-quantiques
chiffrements à clés publiques
résilientes à l'agorithme de Shor



solutions logicielles

quelques conséquences transversales
pour les régulateurs

architectures de systèmes et vie privée

qualité de service et verticalisation du marché

cybersécurité des infrastructures