



prospective numérique et régulation des télécoms

olivier ezratty

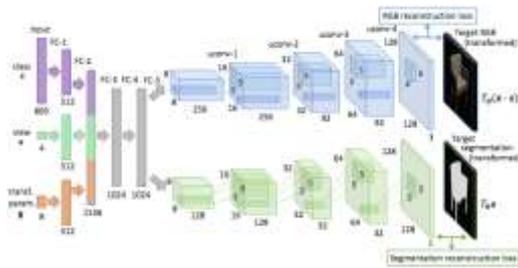
consultant et auteur

olivier@oezratty.net

www.oezratty.net

[@olivez](#)

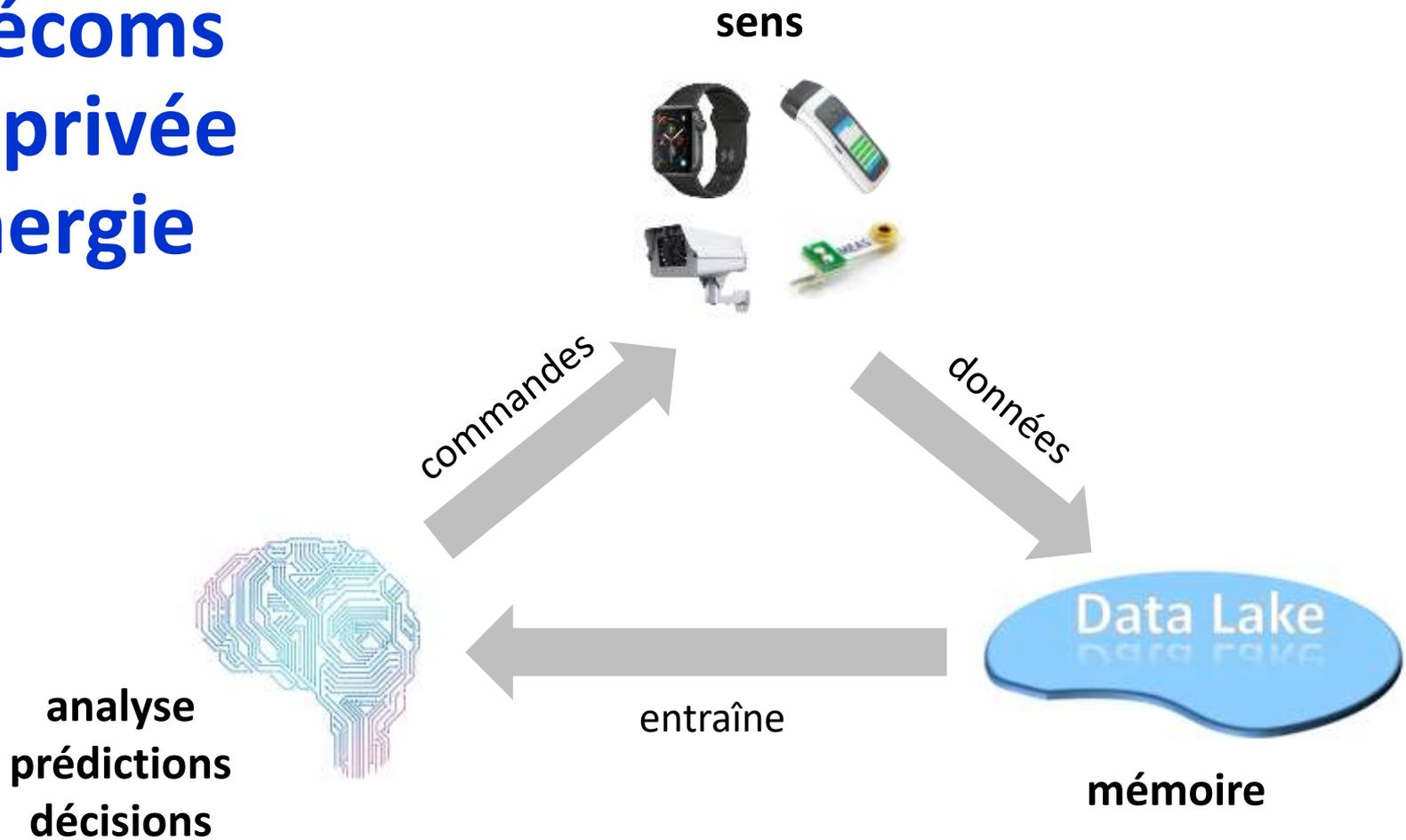
FRATEL, Paris, 23 novembre 2018



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

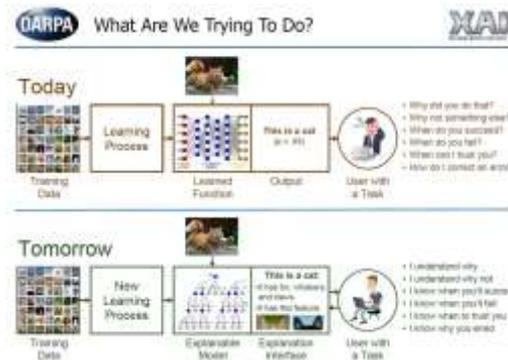
smart city

personnalisation numérique

quelques enjeux de l'IA



données



explicabilité



processeurs

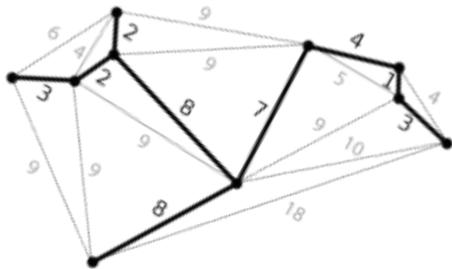


vie privée

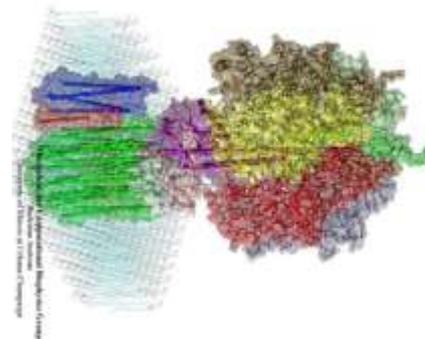


télémédecine

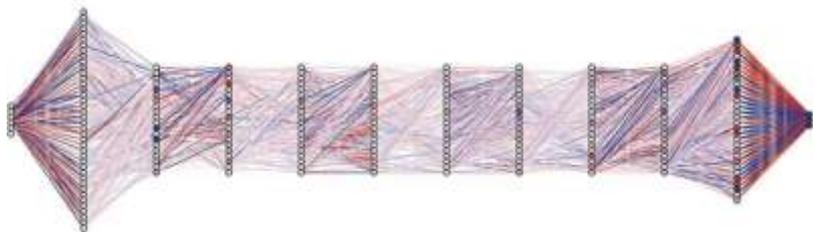
applications du calcul quantique



optimisations combinatoires
trajets, placements, cartes, finance



simulations moléculaires
matériaux et biologie



intelligence artificielle
machine learning et deep learning

```
44 988 956 872 684 695 711 909 595 061 757 551 737 391 461 381 495 437 962 032 535 214 :  
847 417 212 499 752 572 232 401 732 123 638 539 143 471 977 710 243 318 508 178 915 :  
016 041 310 810 028 749 680 395 948 695 236 435 887 854 444 086 897 885 594 538 713 :  
228 936 606 776 470 635 385 948 772 950 847 349 789 474 010 570 972 468 331 714 191 :  
425 331 349 515 850 718 358 938 779 081 862 288 937 248 229 481 122 957 649 663 638 :  
693 717 318 212 628 476 797 261 511 198 103 510 310 449 611 859 242 271 813 366 566 :  
997 130 602 961 939 610 490 851 433 975 035 584 182 642 678 405 161 190 698 336 347 :  
929 112 811 425 354 268 385 653 335 910 754 799 140 572 752 605 907 751 000 463 584 :  
653 690 396 162 388 451 026 377 547 259 579 743 647 906 554 252 830 020 138 218 006 :  
943 421 190 175 143 130 541 480 857 851 924 532 107 288 336 106
```

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.

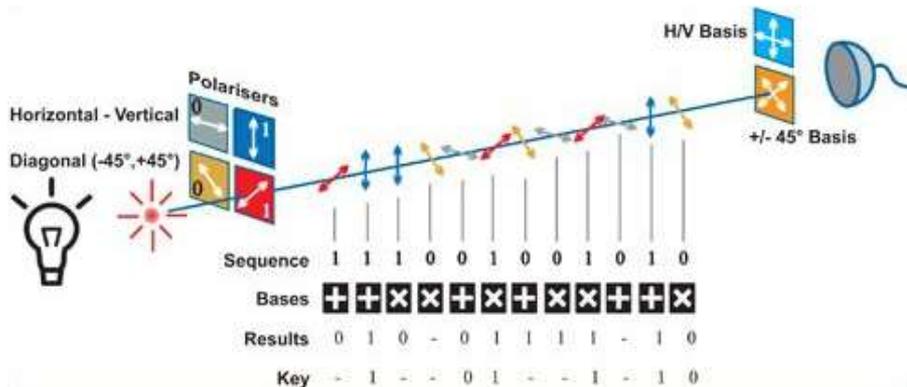
by Emerging Technology from the arXiv November 8, 2017

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

Table 4. Risks to Blockchain Architectures from Quantum Computing

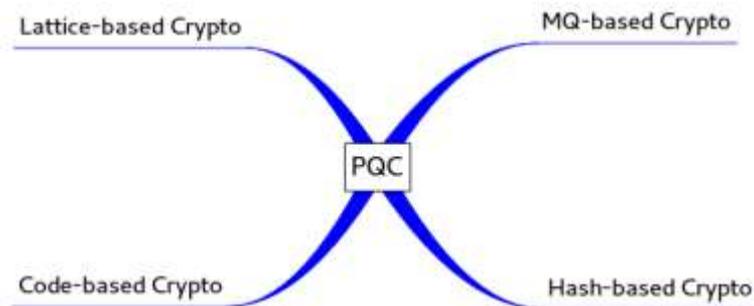
	Transactions	Data on Blockchain	Software on Blockchain
Read historical records without authorization	No (blockchains are intended to allow access to transaction information)	No, unless confidential and secured with vulnerable cryptography	No, unless confidential and secured with vulnerable cryptography
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'algorithme 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