le cnam
Conservatoire national
des arts et métiers

Qu'entend-on par technologie *blockchain* et quelles perspectives pour l'industrie financière ?

Alexis Collomb – Lucas Léger – Klara Sok
SciChain Lab - Cnam

Séminaire sur les « Technologies financières avancées »
ASPROM
12 octobre 2016

Introduction (1/2)

- La technologie « blockchain », également décrite par certains comme la technologie des registres distribués, fait aujourd'hui l'objet d'un intérêt constant dans les médias ;
- Tous les acteurs financiers s'y intéressent, les (ré)assureurs également ; et au-delà, la plupart des acteurs de l'économie numérique et même certaines branches industrielles se penchent sur son applicabilité au sein de leurs secteurs ;
- Les grands principes de cette technologie sont essentiellement dérivés du papier séminal de Satoshi Nakamoto (2008) et du protocole Bitcoin ;
- Initialement la Blockchain désigne simplement la « chaîne de blocs » contenant les informations du réseau Bitcoin, un recueil de toutes les transactions passées sur le réseau depuis son origine ;

Introduction (2/2)

- Puis, avec l'émergence de nouveaux réseaux et protocoles inspirés du Bitcoin, la *blockchain* devient une synecdoque (une métonymie qui consiste à remplacer le tout par la partie) ;
- Plan :

  Qu'entend-on par technologie *blockchain* ?

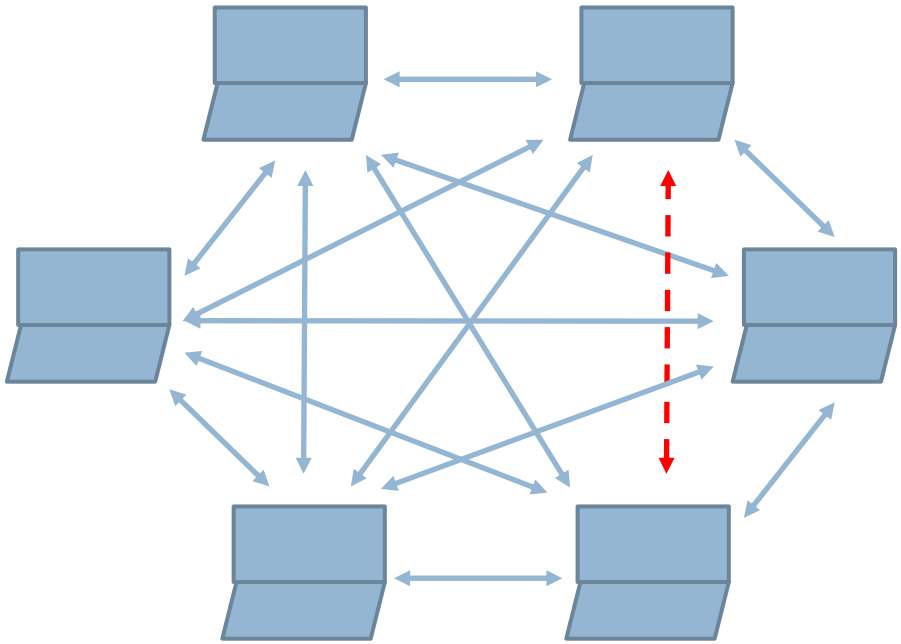
  Sur quelles modalités peut-on jouer ?

  Quelles sont les différentes blockchains aujourd'hui ?

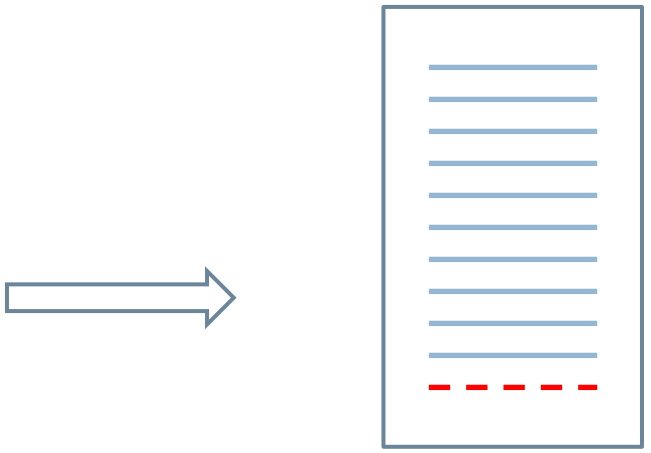
  Scénarios d'intégration dans l'industrie financière et l'assurance

Comment s'accorder sur l'ensemble des transactions d'un réseau, et en garder trace ?

Réseau pair-à-pair



Registre de transactions



Pourquoi le papier fondateur du protocole Bitcoin est-il si important ?

- **Le Bitcoin est la première crypto-monnaie mise en circulation sans l'intervention d'un tiers intermédiaire ;**
- Le développement des crypto-monnaies date de plusieurs décennies, (notamment ecash, DigiCash menées par David Chaum (1981, 1983). Cependant, aucune d'entre elles n'avait encore trouvé de moyen de se passer d'un tiers de confiance (plateforme, registre centralisé des transactions) jusqu'au Bitcoin ;
- Le tiers de confiance était indispensable pour vérifier que des unités de monnaie numérique n'avait pas déjà été dépensées ; un problème qui ne se pose pas avec la monnaie papier ;
- **Satoshi Nakamoto (un pseudonyme) a proposé dans son livre blanc de 2008 la première solution effective au problème de "double-dépense".**

Quels étaient les concepts existants sur lesquels s'est appuyé le protocole Bitcoin ?

- **Les fonctions de hachage cryptographique**, ou **cryptographic hash functions**, qui ont été rendues possibles par le travail novateur de Diffie et Hellman intitulé *New directions in cryptography* (1976) présentant le concept de cryptographie à clé publique
- **Le mécanisme d'enchaînement chiffré des blocs**, ou **cipher block chaining (CBC)**, détaillé dans FIPS PUB 46 (US Federal Information Processing Standards Data Encryption Standard) et approuvé comme norme fédérale (U.S.) en 1976, qui a été développé conjointement par IBM et la National Security Agency (NSA) dans les années 70
- **La preuve de travail**, ou **proof-of-work**, qui a été introduite par Cynthia Dwork et Moni Naor dans un rapport publié en 1993, *Pricing via Processing or Combatting Junk Mail*, où elles proposent de combattre le *spam* (courrier indésirable) en aug- mentant son coût. "L'idée principale est d'obliger un utilisateur à résoudre une fonction suffisamment difficile mais pas insoluble avant d'accéder à la ressource, ce qui décourage une exploitation futile ou malicieuse [de la ressource]." Adam Back a poussé le concept plus loin avec son système *proof-of-work* **Hashcash** dont le but est de limiter le *spam* et les attaques DoS (*denial-of-service* ou par déni de service)
- **Le mécanisme de compression par l'arbre de Merkle,** ou **Merkle Tree compression mechanism (**1979). Il est utilisé pour stocker et vérifier un grand volume de données efficacement et de manière sécurisée, et employé par le protocole Bitcoin pour calculer la racine de Merkle de toutes les transactions contenues dans un bloc de données
- **L'horodatage**, ou **timestamping,** qui est une pratique séculaire dans sa forme physique. Son avatar numérique a été mis au point dans les années 90 pour les besoins des protocoles de sécurité informatique (Une, 2001)
- **La technologie pair-à-pair,** ou **peer-to-peer (P2P) technology**, dont la mise en application par Shawn Fanning en juin 1999 pour la plateforme de partage de fichiers audio Napster est bien connue

Principales caractéristiques du réseau Bitcoin (1/2)

- **Un réseau distribué et décentralisé à la place d'une autorité centrale** - Notons qu'une clé privée est générée par une fonction aléatoire sécurisée de façon cryptographique de 256 bits. Ce n'est pas anodin. La probabilité que deux utilisateurs finissent par avoir la même adresse est ainsi quasi nulle, malgré le fait que ces adresses soient générées de façon décentralisée
- **Un système pseudonyme** - Le réseau Bitcoin est souvent critiqué du fait qu'il permette à ses utilisateurs d'être anonymes, caractéristique perçue comme facilitant le blanchiment d'argent et l'éva- sion fiscale. Il est important de comprendre que chaque nouvelle adresse bitcoin générée est dérivée d'une clé publique, elle-même résultant d'une clé privée via une transformation cryptographique. Et donc remonter de l'adresse bitcoin à son proprié- taire n'est pas simple, même si ce n'est pas non plus impossible…
- **Irréversibilité des transactions** - Cet aspect de la DLT est à la fois perçu comme un avantage et la source de nombreuses critiques. Une fois validée dans la Blockchain, une transaction bitcoin ne peut pas être annulée. Ce système limite le risque que des clients malveillants annulent leur transaction alors qu'ils ont reçu le bien ou service vendu. En un sens, ce système est une façon d'éliminer potentiellement le risque de contrepartie, puisqu'une transaction ne sera validée qu'à condition que l'acheteur payant en bitcoins ait effectivement les fonds disponibles à transférer au vendeur de biens ou services.

Principales caractéristiques du réseau Bitcoin (2/2)

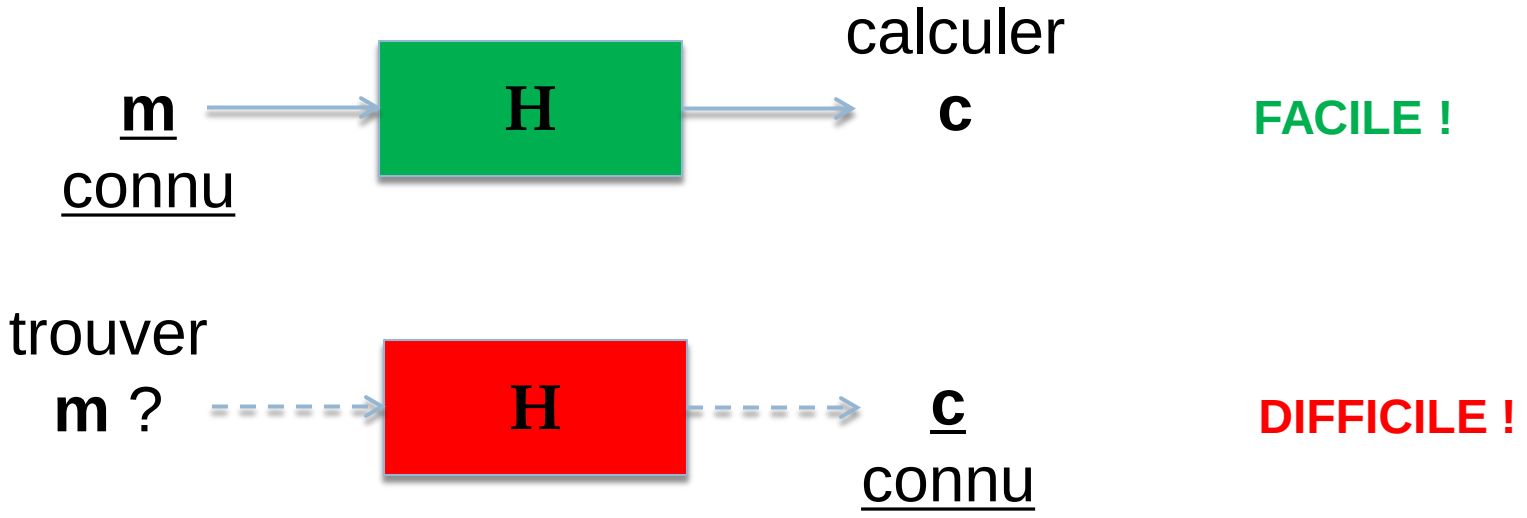
- **Une génération monétaire programmée et limitée** - Le Bitcoin est une crypto-monnaie dont la génération est déterminée à l'avance et dont le montant total est limité à 21 millions d'unités. C'est pourquoi le minage de bitcoins, rémunéré par ces nouvelles unités créées est souvent comparé à l'extraction aurifère dont les ressources en or sont limitées et dont le coût marginal d'extraction augmente avec le temps : le travail d'extraction aurifère devient de plus en plus difficile, et de plus en plus coûteux, alors que les réserves de minerai diminuent
- **Cryptographie -** utilisée à différents niveaux. Au sein du protocole Bitcoin, des procédés cryptographiques sont utilisés pour : (i) générer les clés publiques à partir des clés privées par l'utilisation de courbes elliptiques de chiffrage, à partir du standard secp256k1 tel que défini par le *National Institute of Standards and Technology* (NIST) ; (ii) calculer l'adresse bitcoin de la clé publique par un double hachage de cette dernière, via la fonction à sens unique SHA256 puis RIPEMD160 ; (iii) fournir une signature digitale qui sera utilisée dans un script débloquant la transaction permettant le transfert des fonds vers une adresse bitcoin spécifique ; (iv) calculer l'empreinte (*hash*) d'un bloc valide en faisant varier un *nonce* – étape clé du "minage" ; (v) dans d'autres situations où des empreintes doivent être calculées, notamment lors de la génération de la racine de Merkle d'un ensemble de transactions
- **Mécanismes de consensus et d'authentification** - Le protocole Bitcoin a permis de résoudre un problème ancien en informatique distribuée qui est le problème des généraux byzantins (Lamport et al., 1982). La *proof-of-work (PoW)*, ou preuve de travail (utilisée pour le minage bitcoin), la *proof-of-stake (PoS)*, ou preuve de participation, la *zero-knowledge-proof*, ou preuve à divulgation minimale sont différents paradigmes d'authentification de la validité des transactions utilisés pour établir un consensus sur lequel repose l'immuabilité de la chaîne de blocs

Comment éviter le problème de la double dépense ?

- Ce problème n'existe pas avec le *cash* que nous connaissons ;
- Si on représente électroniquement une unité de compte, un payeur pourrait payer plusieurs fois différents receveurs ;
- La solution : le registre distribué des transactions est visible par tous et il sera (pratiquement) impossible de le modifier, ou d'y ajouter une information qui ne soit pas consensuelle (à très court terme) ;

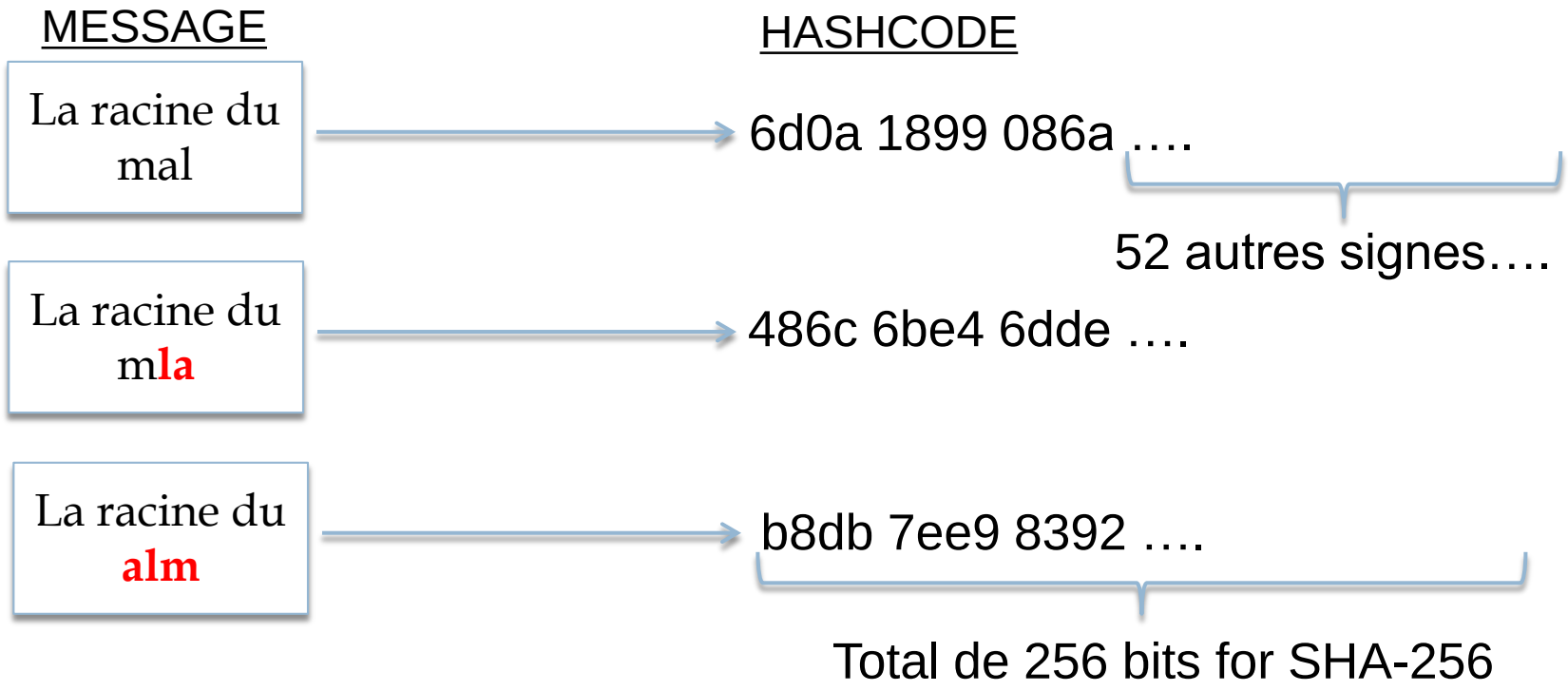
Fonction de hachage (1/2)

- Les fonctions de hachage transforment un message m (un document de taille arbitraire) en un code c ;
- Elles sont quasiment impossible à inverser : si l'on connaît m, c et l'agorithme H, on peut facilement vérifier que H(m)=c ; cependant, si on connaît c et H, trouver m est très difficile ;



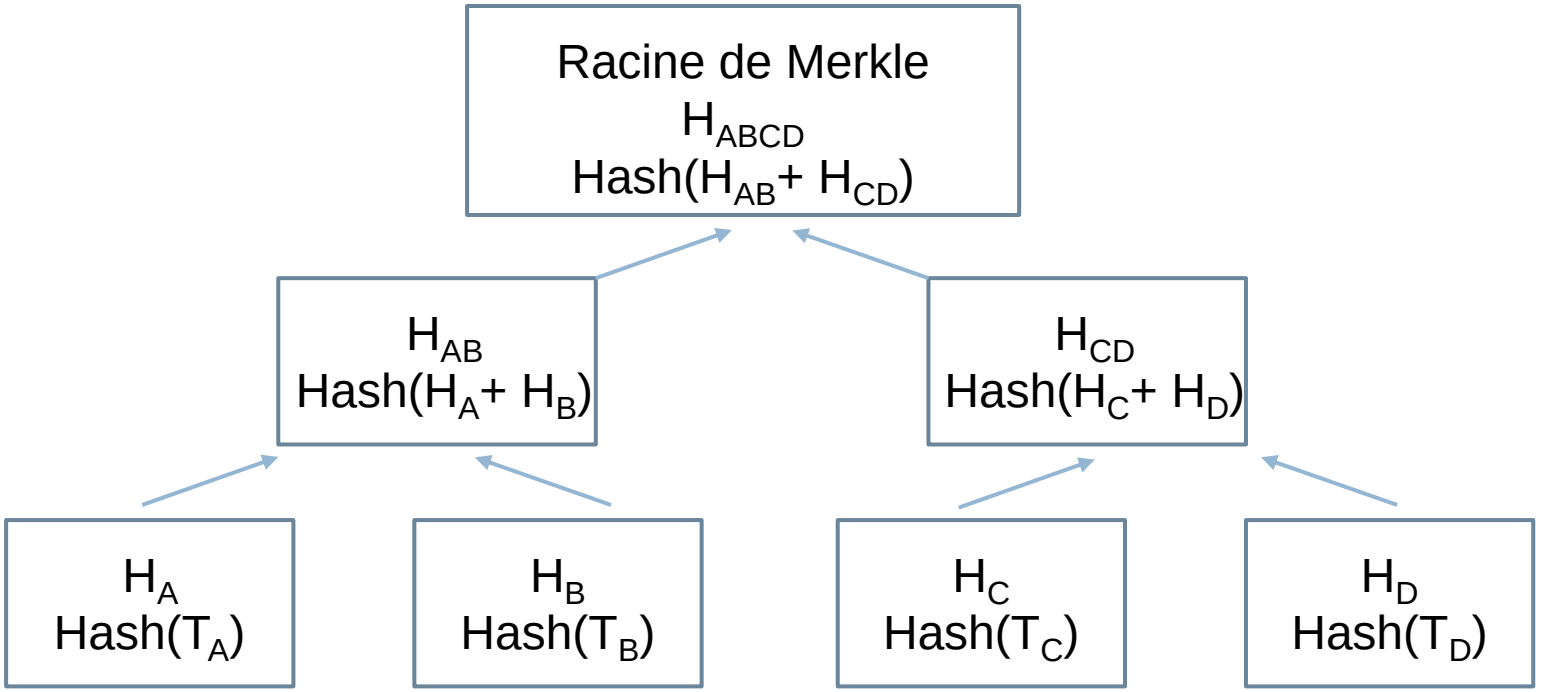
Fonction de hachage (2/2)

- Les fonctions de hachage sont très sensibles aux changements dans le message entrant



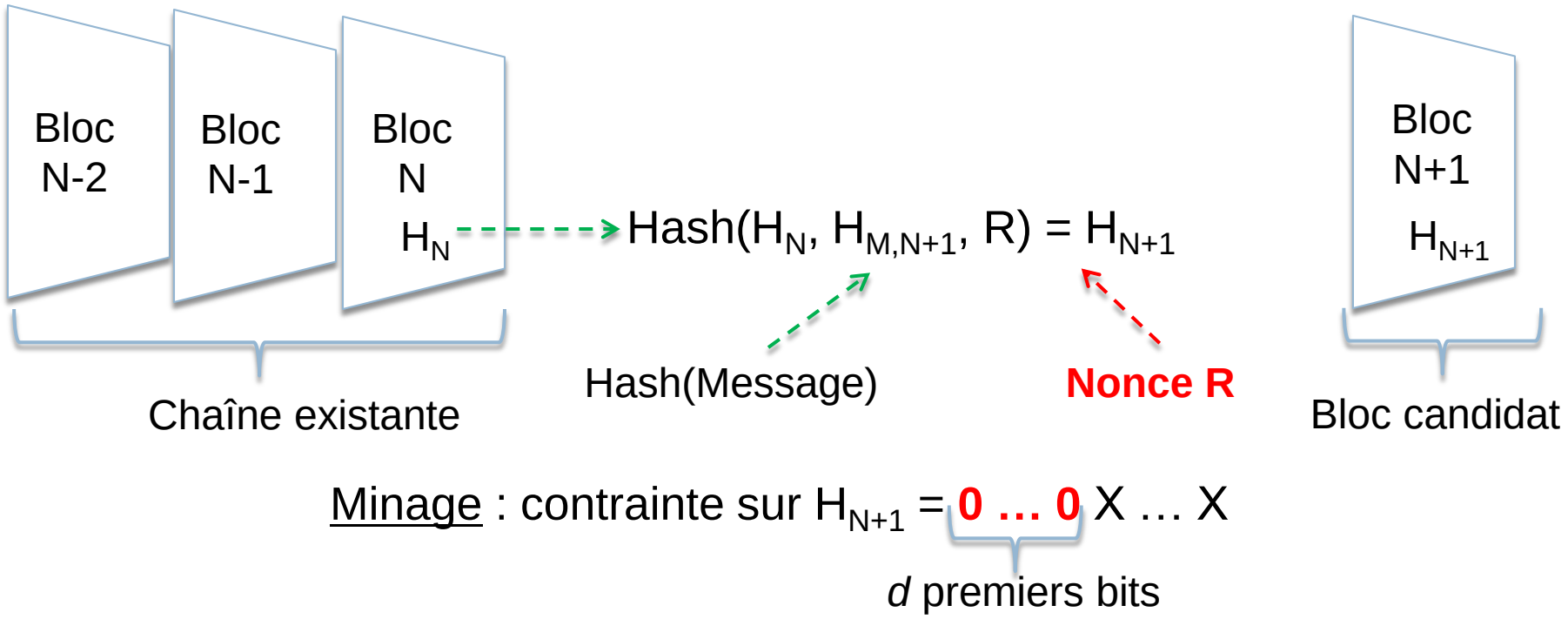
- Le protocole Blockchain utilise l'encodage *Secured Hash Algorithm (SHA)* qui produit un hachage de 256 bits (d'où SHA-256). Il s'agit d'un standard *FIPS (Federal Information Processing Standards)* validé par l'Institut National des Standards et Technologies (*National Institute of Standards and Technology - NIST*)

Utilisation des fonctions de hachage (1/3)
Calcul d'une racine de Merkle



- Une racine de Merkle permet de calculer en cascade une signature digitale d'un bloc d'informations, et donc de vérifier rapidement si des informations contenues dans le bloc ont été modifiées.

Utilisation des fonctions de hachage (2/3)
Ajout d'un nouveau bloc à la *blockchain* et minage



Minage : contrainte sur H_{N+1} = **0 … 0** X … X

d premiers bits

- Pour ajouter un nouveau bloc à la chaîne, un "mineur" aura besoin de trouver la nonce R tel que le hash du bloc candidat commence avec un certain nombre *d* de bits à 0 ;
- Cela implique que seulement 1 des 2^d essais fonctionnera, et cela prend du temps à résoudre…
- ***Notons que le contenu du message de transaction peut être ce que l'on veut ; ainsi la valeur du protocole Blockchain va bien au delà du Bitcoin et est ouvert à de nombreuses autres applications !***

Utilisation des fonctions de hachage (3/3)
Génération des clés et des adresses

- Comment s'assurer sans tiers de confiance centralisateur qu'il n'y a pas de collision d'adresse ?
- On génère une clé privée -> cryptographie sur les courbes elliptiques

  -> clé publique -> RIPEMD160(SHA256(.))

  -> Hash clé publique (160 bits) -> EncodageBase58(.)

  -> Adresse Bitcoin
- Nombreuses possibilités : 2^{256} de l'ordre de 10^{77} (environ 10^{80} atomes dans l'univers visible) ; 2^{160} de l'ordre de 10^{48} (environ 10^{50} atomes sur Terre).

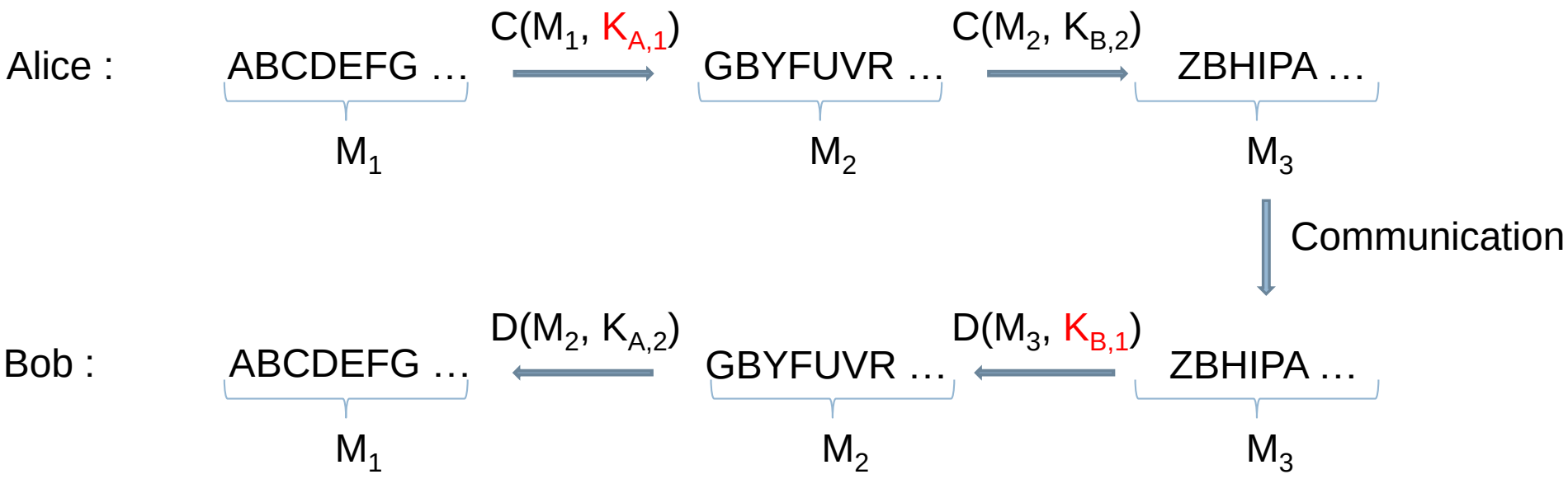
Cryptographie asymétrique (1/2)

- Le principe du chiffrement asymétrique est d'avoir 2 clefs :
  i. Quand l'utilisateur encode avec la première clef (K_1), il peut décoder avec la deuxième clef (K_2) ;
  ii. Quand l'utilisateur encode avec la deuxième clef (K_2), il peut décoder avec la première clef (K_1) ;
- On a donc $\mathbf{D}(\mathbf{C}(M, K_2), K_1) = M$ et $\mathbf{D}(\mathbf{C}(M, K_1), K_2) = M$;
- Asymétrie : une clé est gardée secrète et l'autre est rendue publique.
- Cela permet d'avoir des signatures digitales et des communications authentifiées entre membres du réseau.

Cryptographie asymétrique (2/2)
Communication authentifiée

Clés d'Alice : $K_{A,1}$ (privée) ; $K_{A,2}$ (publique) ;

Clés de Bob : $K_{B,1}$ (privée) ; $K_{B,2}$ (publique) ;



Du Bitcoin … à la technologie blockchain (et à la technologie des registres distribués, alias "DLT")

Comment passe-t-on du Bitcoin à la « technologie blockchain » et des registres distribués ?

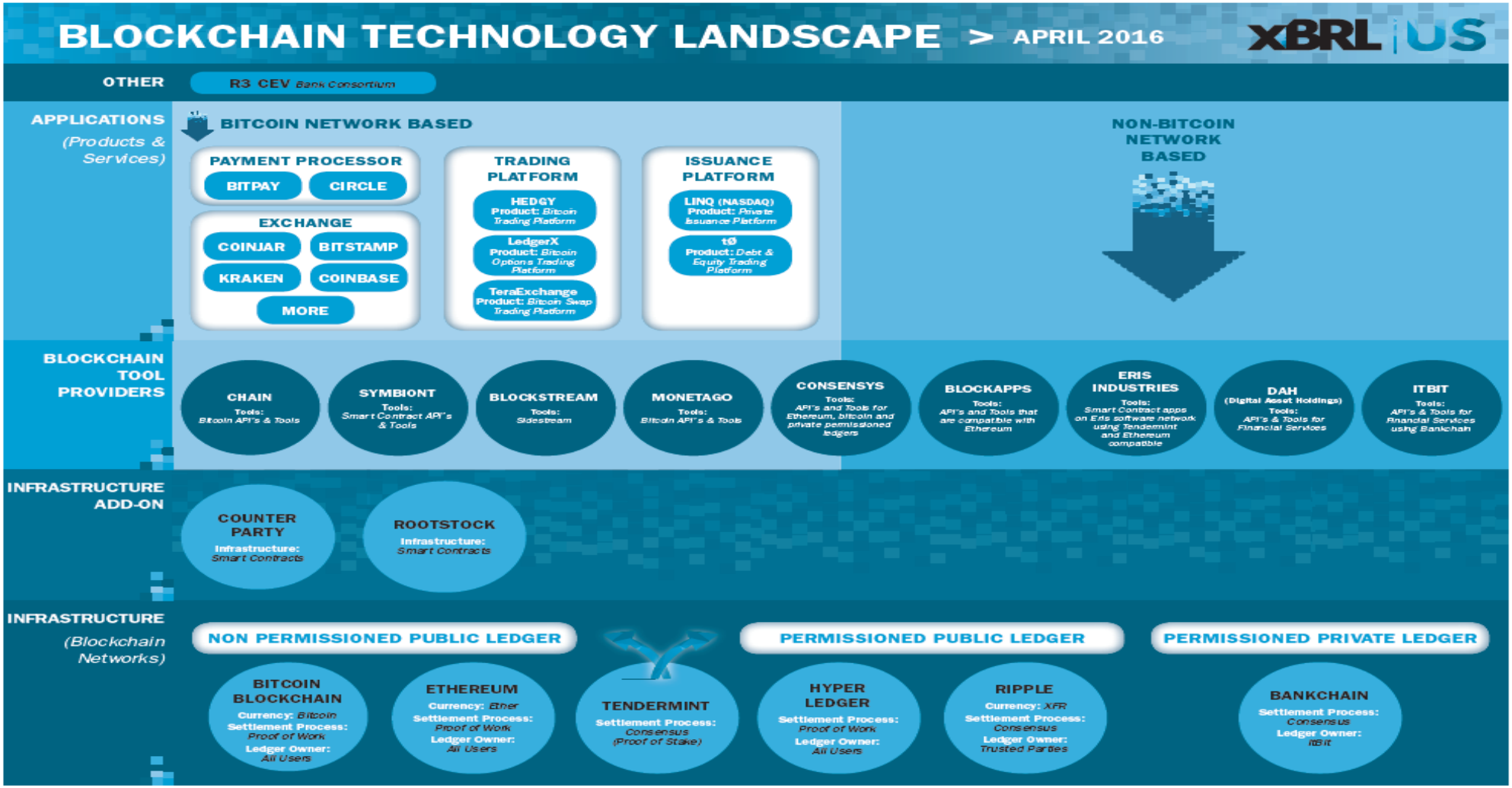
En jouant sur certaines modalités…

- **Chaines privées ou semi-privées** – une hérésie pour certains (certains bitcoiners de la première heure considérant qu'un réseau contrôlé par une minorité est exactement ce qui doit être évité) mais un vif intérêt de la part des grandes entreprises réglementées (gains de productivité par une plus grande efficacité des systèmes d'information et de gestion des transactions, chaînes de consortium, …)
- Inclusion de tout type d'**actif numérique** – utilisation de **smart contracts** permettant la création d'applications decentralisées (**Dapps**) et d'organisations autonomes distribuées (**DAOs**), entreprises autonomes distribuées, sociétés autonomes distribuées (Swan, 2015)
- Un **smart contract** est un "protocole informatique de gestion des transactions qui exécute les termes d'un contrat. Ses objectifs généraux sont de satisfaire les conditions contractuelles communes (telles que les termes de paiement, les privilèges, la confidentialité, ou même la mise en vigueur), de minimiser le risque de dommage intentionnel ou accidentel, et de minimiser le besoin d'intermédiaires de confiance. **D'un point de vue économique, ils visent notamment à diminuer les pertes liées à la fraude, l'arbitrage, les coûts de mise en place et les autres coûts de transactions" (Szabo, 1994)**

Modalités d'ajustement

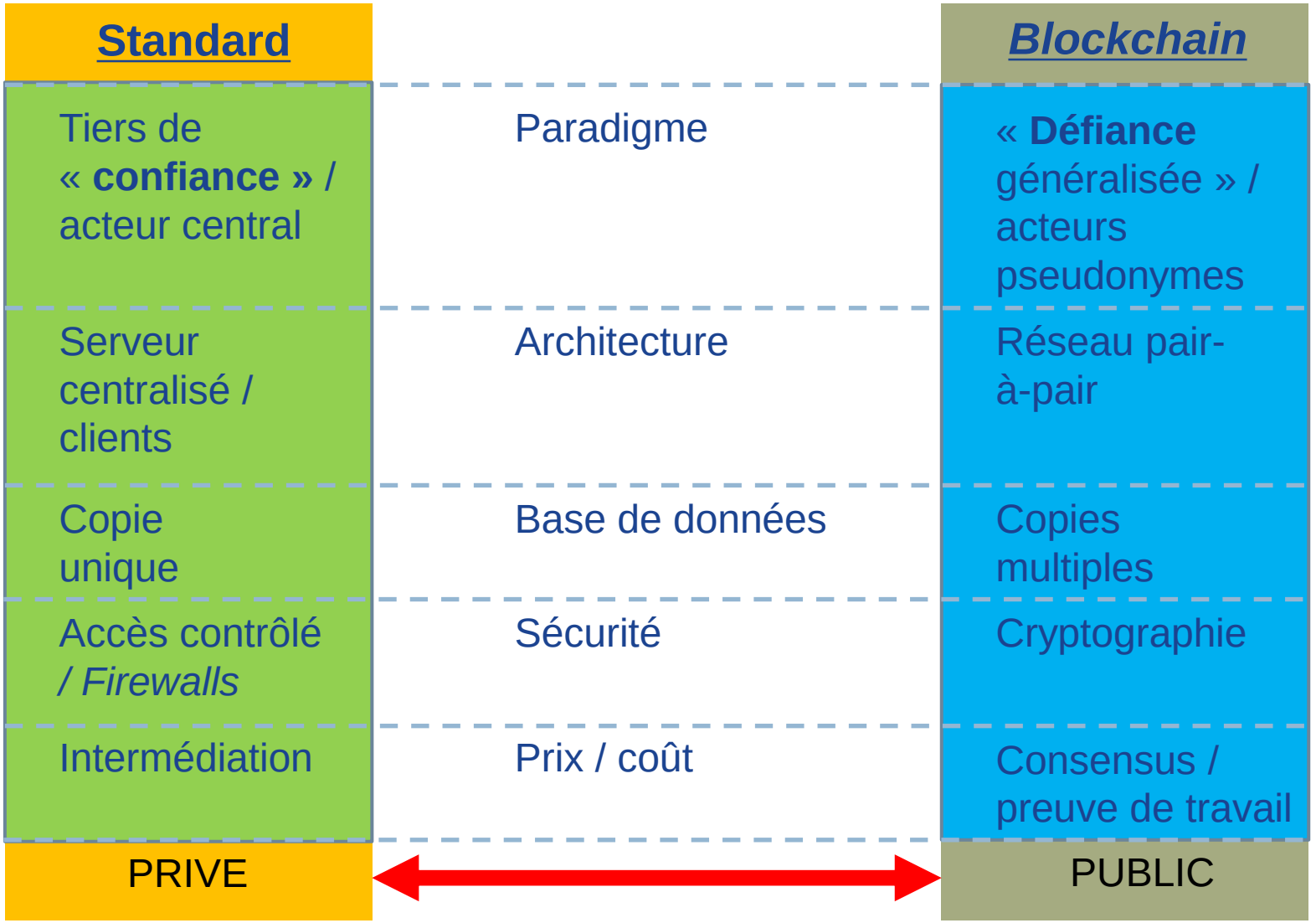
- Nœuds d'authentification : autorisés ou libres ; droits d'accès en lecture ou en écriture ;
- Quel protocole de consensus ? Preuve de travail (*proof of work*) ; preuve de participation (*proof of stake*) ; preuve à divulgation nulle (*zero knowledge proof*) ;
- Quel language de programmation ? Complet au sens de Turing ou non ? Bitcoin non, Ethereum oui… Implications sur la stabilité du réseau ;
- Quelles données veut-on stocker sur la *blockchain* ?
- Quel degré de confidentialité recherché pour les utilisateurs ? Données chiffrées ou non ? Non pour le réseau Bitcoin, oui pour d'autres réseaux (e.g. Monero) ;
- Quel rôle pour une *blockchain* donnée ? Principal ou périphérique (*sidechain*) ?
- Comment augmenter le débit du réseau ? En utilisant une *blockchain* de référence pour y stocker les résultats nets d'opérations faites sur un autre réseau (e.g. le Lightning Network pour la Blockchain).

Il y a eu une rapide évolution du secteur …



Source : XBRL.US via: http://fintechnews.sg/2305/blockchain/landscape-blockchain-companies-financial-services/

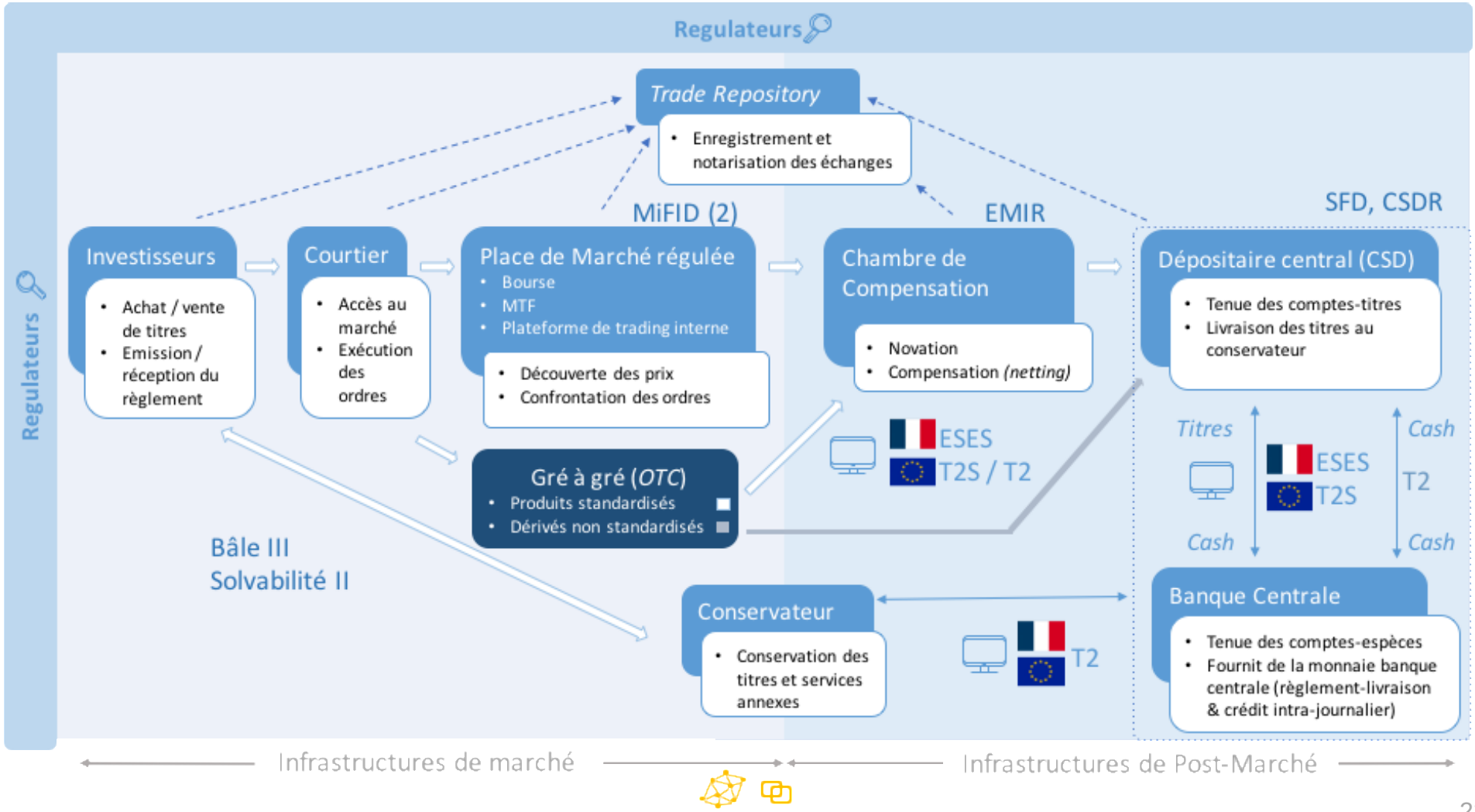
… et un nouveau modèle transactionnel



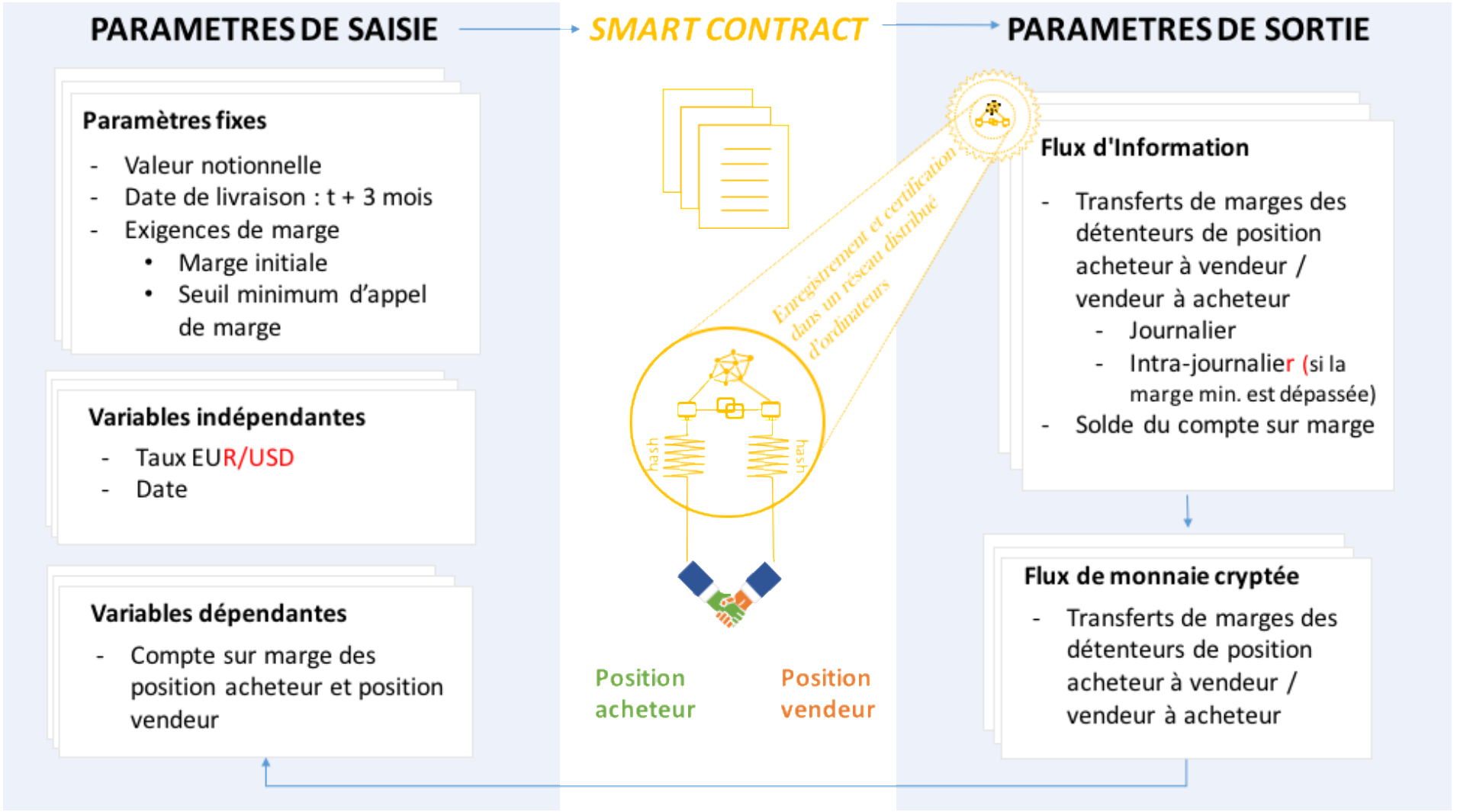
Que signifie la technologie des registres distribués (DLT) pour le monde de la finance, et au-delà ?

- **Marchés financiers : La DLT est-elle à l'origine d'un nouveau paradigme d'efficacité ?** Dans quelle mesure la DLT, en tant que moyen de garder et de transférer la propriété d'actifs numériques, modifie-t-elle la chaîne de valeur des marchés financiers ?
- **Un rêve de** "traçabilité quasi-totale et immuable de toutes les transactions, pour tout type d'actif numérique avec un règlement-livraison instantané, une gestion automatique des appels de marge et des fonctions de reporting et de conformité intégrées facilitatant la gestion des risques et le travail des régulateurs…"
- **La réalité d'aujourd'hui** : une infrastructure post-marché complexe, et de nombreux intérêts d'acteurs historiques rendant difficile un changement rapide et massif de l'infrastructure ;
- Au delà des marchés financiers, la technologie blockchain c'est probablement de nombreuses applications pour la **finance d'entreprise** (ex.: vote électronique des actionnaires une situation de fusion & acquisition), le ***trade finance***, l'**assurance** (e-constats, mécanismes de mutualisation automatisés) ;
- **Inclusion financière** (c.2,5 Mds d'individus sans compte en banque) ;
- **Politique monétaire** (revenu universel, etc.)**.**

Un vecteur de simplification pour l'infrastructure post-marché ?

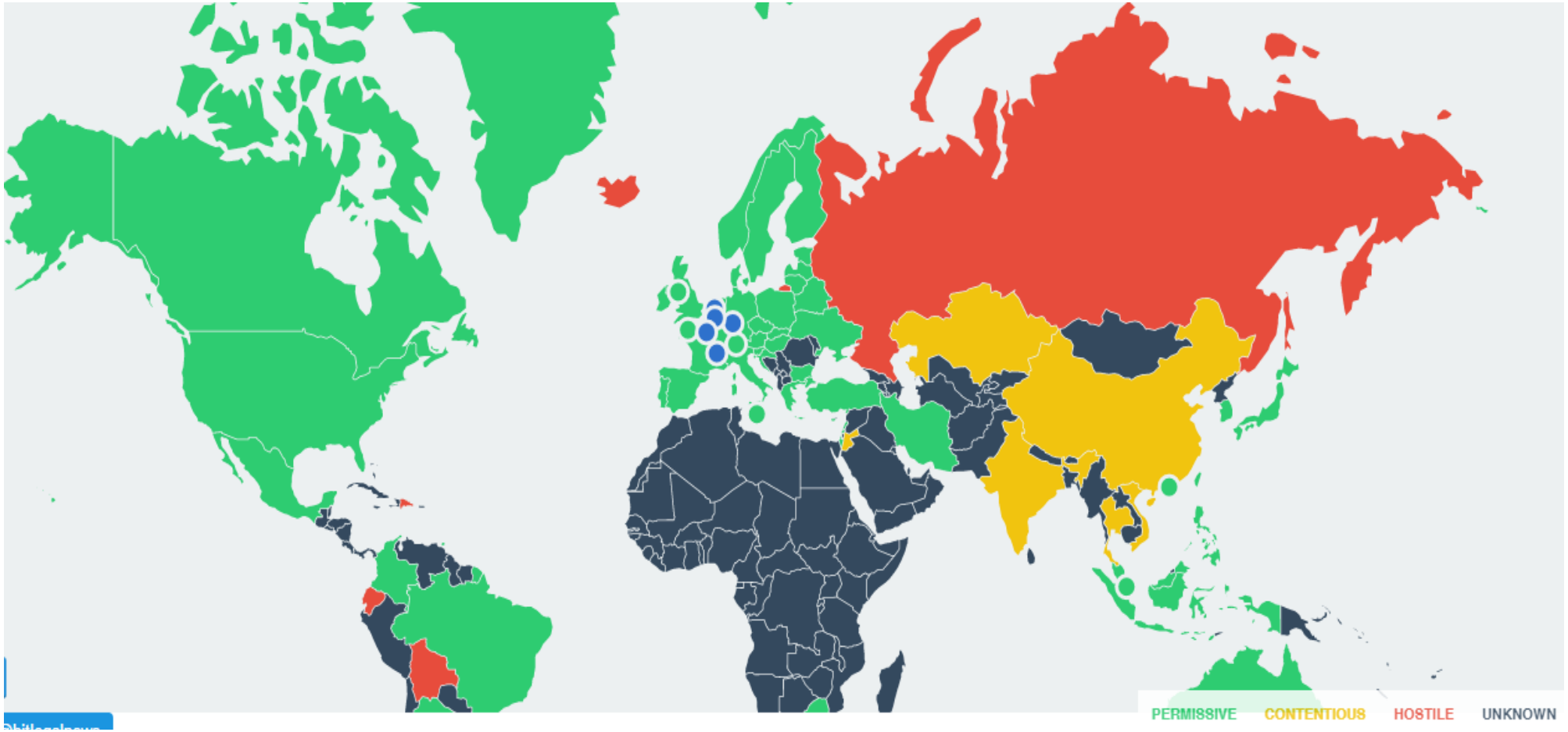


Vers une infrastructure financière régulée par des *smart contracts* ?



Quid de la réglementation aujourd'hui ? (1/2)

- **Commençons par le Bitcoin… Règlementation variée, parfois embryonnaire ou inexistante...**



Source: bitlegal.io

Quid de la réglementation aujourd'hui ? (2/2)

- Des 74 nations pour lesquelles de l'information existe, 62 ont permis le développement du Bitcoin ;
- Mais même au sein de certains pays, les différentes instances officielles ne sont pas forcément d'accord sur la définition (juridique) d'un bitcoin (e.g. Etats-Unis) ;
- Et c'était pour le bitcoin ; pour la technologie blockchain et les organisations décentralisées quelle permet, c'est encore plus flou ; il n'y a quasiment rien ;
- Une résolution récente du parlement européen (adoptée le 25 mai 2016) a appelé à une approche réglementaire proportionnée, afin d'une part de ne pas inhiber l'innovation à ce stade en créant des coûts superflus, tout en permettant d'autre part de prendre au sérieux les défis réglementaires qu'un développement rapide de la technologie pourrait poser ;
- **Cette résolution a par ailleurs souligné que certaines réglementations clés comme EMIR, CSDR, SFD, MiFID/MiFIR, AIFMD pour en citer quelques-unes, pourraient fournir un cadre juridique approprié pour les activités proposées. Mais que de nouvelles réglementations taillées sur mesure pourraient aussi être envisagées.**

Résolution européenne (1/2)
Opportunités de la technologie

Le Parlement européen a souligné que les monnaies virtuelles et la technologie blockchain/des registres distribués (DLT) ont le potentiel de « contribuer positivement au bien commun et au développement économique, notamment dans le secteur financier », en :

- réduisant les coûts opérationnels et de transactions pour les paiements, en particulier transfrontaliers :
- réduisant le coût d'accès au système financier, et en permettant donc plus d' « inclusion financière » (sans nécessairement de compte en banque traditionnel) ;
- favorisant la robustesse et la vitesse des systèmes de paiement, et des échanges de biens et de services ;
- permettant des systèmes combinant facilité d'utilisation, coûts de transaction et d'exploitation faibles, et confidentialité (sans pour autant permettre une anonymité totale).

Résolution européenne (2/2)
Risques de la technologie

Cependant les monnaies virtuelles et la technologie blockchain/des registres distribués (DLT) comportent également des risques qu'il faudra suivre attentivement, notamment :

- l'absence de structures de gouvernance identifiées et stables ;
- la grande volatilité des monnaies virtuelles et le potentiel de bulles spéculatives qu'elles représentent ;
- les sources d'instabilité financière que leurs produits dérivés représentent ;
- leur utilisation potentielle pour le marché noir, le blanchiment d'argent, le financement du terrorisme, la fraude ou l'évasion fiscale, et tout autre forme de financement d'activités criminelles ;
- leur coût énergétique élevé dans certains cas (e.g. on estime qu'aujourd'hui la consommation du réseau Bitcoin excède 1GW).

Comment faut-il réguler la technologie blockchain ?

- Si l'environnement Bitcoin commence à être régulé, ce n'est vraiment pas le cas de tout autre blockchain ;
- Réguler des monnaies virtuelles est très différent de réguler une blockchain du type Ethereum ou NXT, qui peuvent servir de support pour une organisation autonome décentralisée et/ou des mécanismes de gouvernance programmés ;
- Aujourd'hui il n'y a pas de corpus légal autour de la Blockchain (Wright & De Filippi, 2015) ;
- Cela renvoie à un vieux débat sur la réglementation de l'Internet à la fin des années 90s, et à la mise en place de "cyberlaw" (Lessig, 2006) ;
- Va-t-on passer après la ***lex marcatoria*** et la ***lex informatica*** à la ***lex cryptographia*** ? (Wright & De Filippi, 2015) ;
- Il faut distinguer les blockchains (semi-)privées (où une dose de regulation est possible, notamment car les acteurs contrôlant les nœuds du réseau sont eux-mêmes réglementés) des blockchains publiques (où les règles ne s'exécutent qu'à travers le code et ne sauraient être force de loi qu'à la seule condition d'un accord international sur le sujet).

Une technologie à fort potentiel pour des choix collectifs complexes

- Selon Vitalik Buterin dans un récent article sur Medium : « *two agents can agree to both commit to maximize a goal which is the average of the two goals that they previously had. Previously, such concepts were largely science fiction, but now futarchy DAOs can actually do this.* »
- Autrement dit, la technologie blockchain permettrait une articulation très fine entre préférences individuelles et choix collectif, entre objectifs personnels et objectif de groupe. Cette programmation des objectifs se fonde sur des attentes de comportements rationnels qui posent certaines questions, notamment en lien avec des travaux d'économie comportementale qui mettent en évidence certaines irrationalités.
- Plus spécifiquement lié au processus de vote au sein des DAOs
  - Les modèles observés s'appuient sur une règle à la majorité simple (ou apparentée) qui pourrait ne pas suffisamment rendre compte des limites – voire impossibilités – de trouver un choix collectif cohérent à partir des préférences individuelles (paradoxe de Condorcet, théorème d'impossibilité d'Arrow), ou d'éviter les risques de manipulation (Gibbard, 1973 ; Satterthwaite, 1975) ; au passage, la possibilité de prendre en compte les intensités des préférences individuelles offre de nombreuses possibilités pour sortir de ces paradoxes ;
  - Ce contexte serait favorable à l'adoption de comportements stratégiques, de la part de certains investisseurs, contraires à la philosophie horizontale, démocratique et décentralisée souhaitée par The DAO (Mark, Zamfir & Sirer, 2016).

Conclusion (1/2)

- **La « technologie blockchain » est porteuse de promesses selon différentes dimensions** (efficience transactionnelle et réduction des coûts de transaction, gestion facilitée du risque, reporting et tests de conformité automatisés, etc.) ;
- **Elle fournit à la fois un nouveau modèle transactionnel décentralisé dans sa version ouverte et publique, et permet en même temps une accélération de la transformation numérique dans ses versions privée ou semi-privée** ; elle n'attire pas les mêmes acteurs selon les cas (une communauté citoyenne/open source dans le premier cas ; des institutions soucieuses d'améliorer leurs processus transactionnels et de réduire leurs coûts dans le second) ;
- **Comment les différentes blockchains s'intégreront n'est pas encore clair** ; pour l'heure il y a de nombreuses initiatives mais qui restent encore des niches ; la Blockchain du Bitcoin a montré une résilience certaine ; d'autres nombreuses initiatives (Ethereum, etc.) sont en plein développement (Devcon 2 …) ;
- **Pour ceux qui demeurent sceptiques, penser au rapport Théry (et al.) de 1994 sur les autoroutes de l'information** ("[Le] mode de fonctionnement coopératif [de l'Internet] n'est pas conçu pour offrir des services commerciaux …") ;

Conclusion (2/2)

- Des questions clés à garder en tête sur le développement de la technologie :
  i. Passage à grande échelle et accélération du débit ?
  ii. Mise en place d'une « infrastructure blockchain » ? Interopérabilité entre les blockchains (Blockchain, sidechains, etc.) ?
  iii. Etablissement des standards et des normes (à défaut de réglementation) – par qui ? Selon quel timing ?
  iv. La gouvernance et les algorithmes de consensus ;
  v. La propriété et la confidentialité des données ;
  vi. Le rôle et la réglementation du chiffrement ;
  vii. Toutes les autres questions de régulation ;
  viii. La sécurité et la souveraineté ;
  ix. Les modèles économiques et les incitations des différents acteurs.