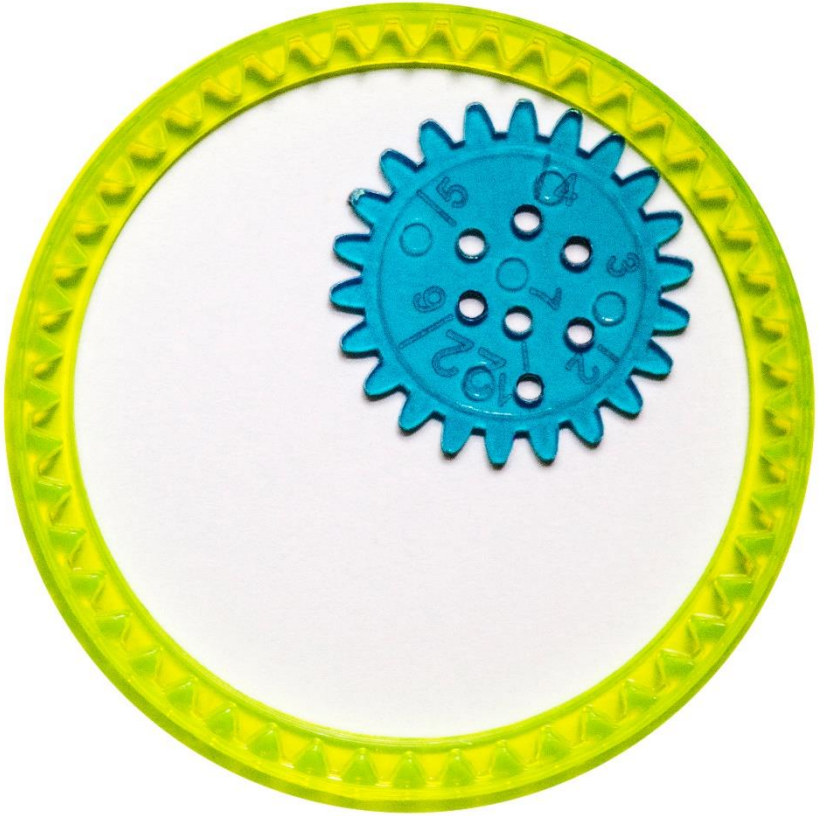
Deloitte.



La Blockchain

Panorama des technologies existantes

Identification de nouveaux cas d’usage Blockchain

7 critères de décision

Processus numérisable ?

Nombreuses parties prenantes ?

Intérêts des acteurs non alignés ?

Multiples acteurs avec droit d’écriture ?

Découplage preuves-données ?

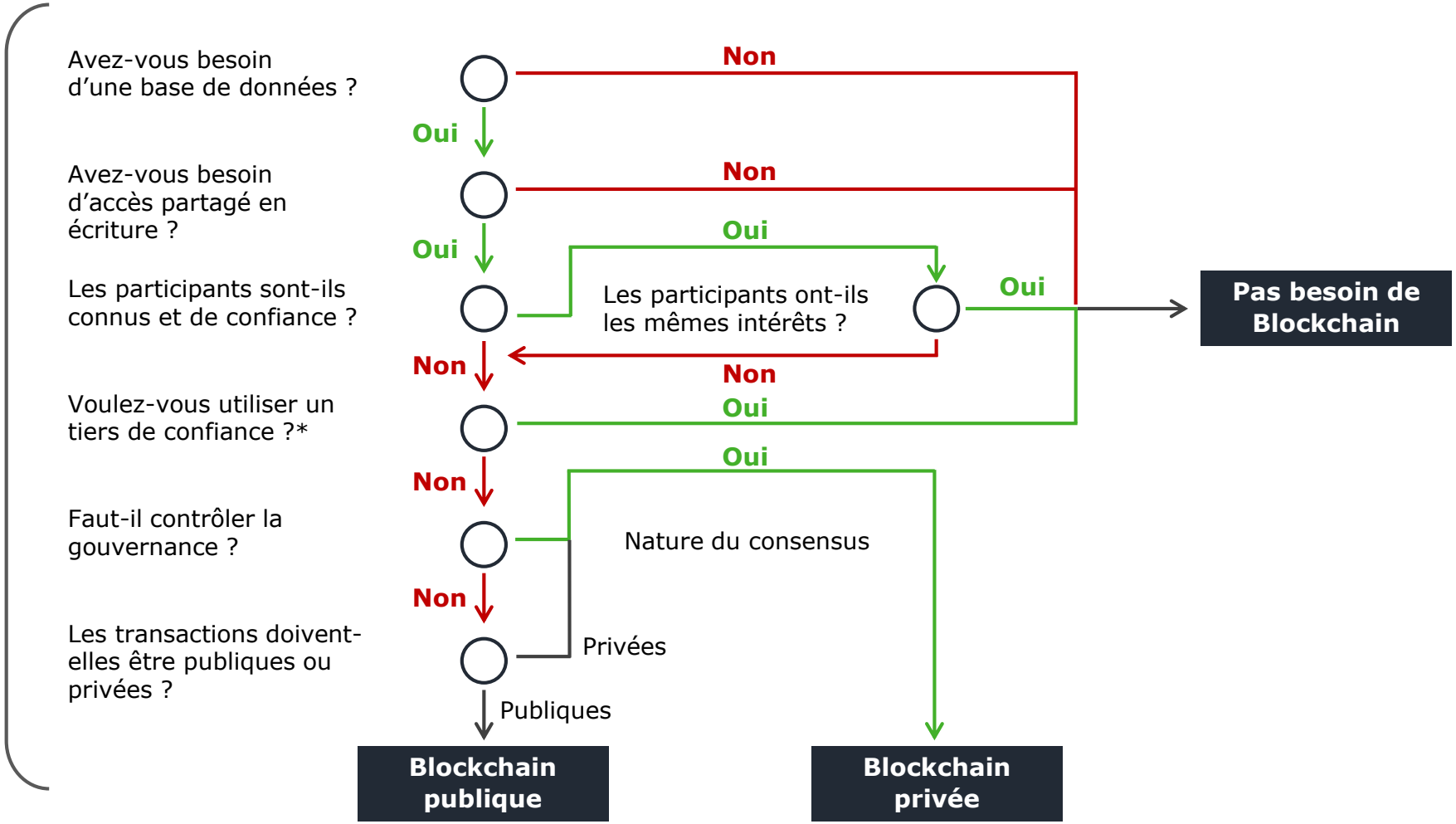
Besoin de conformité ?

Enjeux financiers ?

Les types de Blockchain

Comment construire une stratégie Blockchain?

Avez-vous besoin d'une Blockchain ?



⚠ Tiers de confiance traditionnel déjà existant. Excluant les Oracles qui jouent le rôle de confiance au sein d'une Blockchain.

Les deux approches de la Blockchain

	Blockchain publique		Blockchain privée
Usage	Nous préconisons l'usage d'une Blockchain publique pour gérer des traces simples (hash) pour une piste d'audit. Au-delà des traces simples, la Blockchain publique est moins pertinente compte tenu de son coût de manipulation des données et de ses limites dans la gestion de la confidentialité.		Nous préconisons l'usage d'une Blockchain privée pour gérer des échanges plus riches que de simples traces. L'absence de frais de transaction permet une taille des données stockées plus importante. En outre, la gestion des droits d'accès et de la confidentialité peut être davantage maitrisée.
Sécurité	Plus il y a d'utilisateurs, plus la sécurité de la Blockchain est garantie. Généralement, le consensus sur une Blockchain publique est garanti par la preuve de travail (PoW).		Seuls les nœuds validateurs sont autorisés à valider une transaction. Un consensus de n% (par ex 2/3) des membres validateurs est requis.
Confidentialité	Les données transitent de manière transparente. Sauf divulgation, les détenteurs des adresses sont anonymes (i.e. transactions semi-anonymes).		Seuls les acteurs autorisés de la Blockchain privée ont accès aux transactions.
Scalabilité	Entre 3 et 7 transactions financières par seconde mais une transaction peut contenir plusieurs milliers de hash grâce au processus de « Merklelisation ».		1 000 transactions par seconde, voire plus.
Accessibilité	« Permisionless » : comme internet, accessible à tous.		Accès aux membres du consortium uniquement.

● Fort ○ Faible

Les consensus

	Description	Avantages	Inconvénients
PoW	**Proof of Work** : Preuve de travail. Dans une Blockchain publique, les ordinateurs des mineurs sont mis à disposition pour résoudre un problème mathématique compliqué. Le 1er qui trouve une solution gagne la récompense du prochain bloc de la chaine (12.5 bitcoin ou 5 ether).	• Sécurisé, éprouvé et robuste.	• Très consommateur d'électricité et de matériel informatique.
PoS	**Proof of Stake** : Preuve d'enjeu. Les validateurs de transactions doivent mettre en gage la possession de crypto monnaie pour recevoir une récompense. Si un nœud est malveillant, il peut perdre sa mise en gage au profit des validateurs honnêtes.	• Peu consommateur en ressources énergétiques.	• Peu testé à grande échelle.
PBFT	**Practical Byzantine Fault Tolerant** : Consensus dont la liste des validateurs est connue au départ et peut tolérer jusqu'à 1/3 de nœuds compromis (déconnectés ou malveillants).	• Consensus de groupe rapide et performant. • Pas de fork ou de réorganisation de chaine.	• Chaine privée uniquement.
PoA	**Proof of Authority** : Preuve d'autorité. Consensus dont la liste des validateurs est connue au départ et qui valide à tour de rôle un bloc. Ce type de consensus peut tolérer jusqu'à 49% de nœuds malveillants ou déconnectés.	• Consensus de groupe rapide.	• Chaine privée uniquement. • Fork ou réorganisation de la chaine possible.

Les principales Blockchain 1/2

		Description
	**Bitcoin**	Créé par Satoshi Nakamoto en 2008, Bitcoin est la **Blockchain originelle** dont le consensus repose sur la preuve de travail (**PoW** : proof of work) des mineurs. Elle sert principalement aujourd'hui de valeur refuge numérique. Bitcoin permet aussi de stocker une petite quantité d'information dans chaque transaction (80 octets) de manière immuable. Il est aussi possible d'utiliser Bitcoin pour émettre et faire circuler des jetons (colored coin) pouvant être l'émanation sur la chaine d'un actif sous-jacent (action, titre de propriété, matière première…).
	**Ethereum**	Créé par Vitalik Buterin en 2014, Ethereum permet, au-delà des fonctions de Bitcoin, de créer des contrats intelligents (**smart-contract**), c'est-à-dire des comptes pouvant transporter des ethers (crypto monnaie) pilotés par du code informatique. En 2017, les smart-contract sont principalement utilisés pour l'émission de jetons et les levées de fonds directement sur la Blockchain.
	**Hyperledger**	Hyperledger est une **plateforme open source** de développement de Blockchain. Ce projet, initié en décembre 2015 par la fondation Linux, a été rejoint plus tard par IBM. Le développement s'y fait essentiellement en langage Go.
	**Tendermint**	Tendermint est une plateforme open source de Blockchain permettant l'exécution de smart-contract multi-langages dont l'algorithme de consensus PBFT résiste à la panne, même si 1/3 des acteurs sont malveillants ou déconnectés.
	**Zero Cash**	Z-Cash est une Blockchain permettant les **transactions anonymes** grâce à la technologie cryptographique innovante zk-SNARK. Sur le réseau Z-cash, il existe 2 types d'adresse : les transparentes « t-address » et les protégées « z-addresses ». Les transactions entre les premières sont similaires à celles de Bitcoin, celles qui se font sur la seconde en revanche sont inscrites dans le registre de manière chiffré. un algorithme dit « de preuve à divulgation nulle de connaissance » (zero-knowledge proof) garantit l'intégrité de ces transactions.
	**Tezos**	Après la fructueuse levée de fonds du mois de juillet (200M €), la chaine publique de Tezos sera lancée fin 2017. Tezos est une Blockchain dont le consensus repose sur la preuve d'enjeu (**PoS** : Proof of Stake) à « **gouvernance intégrée** ». En effet, toute proposition d'évolution du code source soumise à un vote réunissant 80% sur un Quorum de 80% des détenteurs de Tez donnera lieu à une mise à jour. De plus, le langage utilisé pour les smart-contract est écrit en Ocaml et permet la **vérification formelle** de la cohérence entre le code compilé et le code source.

Les principales Blockchain 2/2

		Gouvernance	Consensus **PoW** : Proof of work **PoS** : Proof of stake **PBFT** : Practical Byzantine fault tolerant	Nombre de nœuds	Smart contract	Chaine publique (token)	Transaction privée (possibilité)	Date de lancement
	**Bitcoin**	Décentralisée au niveau mineurs	PoW	7 500	× Multisig*	✓ BTC (bitcoin)	×	01/2009
	**Ethereum**	Fondation Ethereum, Méritocratie, mineurs	PoW (*PoS* prévu d'ici 1-2 ans)	35 000	✓ Solidity	✓ ETH (ether)	×	07/2015
	**Hyperledger**	N/A	PBFT	N/A	✓ Go ou Java	×	✓	2016
	**Tendermint**	N/A	PBFT	N/A	✓ Go ou autres	×	×	2016
	**Zero Cash**	Fondation Zcash, mineurs	PoW	850	× Multisig*	✓ ZEC (Z-cash)	✓	10/2016
	**Tezos**	Gouvernance intégrée	PoS	N/A	✓ Ocaml	✓ XTZ (Tez)	×	2018

* Multi-signature : possibilité d'utiliser une adresse nécessitant n parmi m signature(s) pour valider une transaction sortante

Contacts

Julien Maldonato

Associé Conseil
Industrie Financière

+33 1 40 88 70 98

jmaldonato@deloitte.fr

Rémi Foult

Lead développeur
Blockchain

+33 1 58 37 99 24

rfoult@deloitte.fr

Deloitte.

A propos de Deloitte

Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited, société de droit anglais (« private company limited by guarantee »), et à son réseau de cabinets membres constitués en entités indépendantes et juridiquement distinctes. Pour en savoir plus sur la structure légale de Deloitte Touche Tohmatsu Limited et de ses cabinets membres, consulter www.deloitte.com/about. En France, Deloitte SAS est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.

Deloitte fournit des services professionnels dans les domaines de l'audit, de la fiscalité, du consulting et du financial advisory à ses clients des secteurs public et privé, quel que soit leur domaine d'activité. Fort d'un réseau de firmes membres dans plus de 150 pays, Deloitte allie des compétences de niveau international à un service de grande qualité afin d'aider ses clients à répondre à leurs enjeux les plus complexes.
Nos 244 000 professionnels sont animés par un même objectif, faire de Deloitte la référence en matière d'excellence de service.

En France, Deloitte mobilise un ensemble de compétences diversifiées pour répondre aux enjeux de ses clients, de toutes tailles et de tous secteurs – des grandes entreprises multinationales aux microentreprises locales, en passant par les entreprises moyennes. Fort de l'expertise de ses 10 300 collaborateurs et associés, Deloitte en France est un acteur de référence en audit, risk advisory, consulting, financial advisory, juridique & fiscal et expertise comptable, dans le cadre d'une offre pluridisciplinaire et de principes d'action en phase avec les exigences de notre environnement.

PARTENAIRE OFFICIEL
FRANCE2025