

Quel consensus pour les cryptomonnaies ? (2/3)

Rédigé le 23 août 2018 par [Nicolas Perrin](#) / [Bitcoin et autres cryptomonnaies](#), [Crypto Monnaies](#)

Les grandes banques d'investissement se mettent déjà – même indirectement – au négoce du bitcoin. Le consensus choisi par les investisseurs institutionnels sera déterminant.

Demelza Kelso Hays et Mark J. Valek (H&V), les auteurs de la IIIe édition du « Crypto Research Report » d'Incrementum, considèrent que « l'hiver des cryptos » est loin d'être terminé. Cela n'empêche pas pour autant l'investisseur prévoyant de réfléchir à la diversification de son portefeuille de crypto-actifs.

Au total, on dénombre 17 mécanismes de consensus, « quelque chose » qui signifie qu'on s'accorde pour valider les transactions ou blocs. Les cryptomonnaies constituent des enregistrements de transactions sur des registres ouverts et décentralisés. Il faut donc pouvoir se mettre d'accord à distance et sans tiers de confiance. Le rapport recense 17 solutions.

Liste des mécanismes de consensus parmi les 100 premiers crypto-actifs		LCA
Consensus Mechanism	Cryptocurrencies	
Proof of Work	Bitcoin, Ethereum Classic, Syscoin, DigiByte,	
Proof of Stake	NXT, PIVX, Reddcoin, Stratis, Ardor, Neblio,	
Leased Proof of Stake	Waves	
Delegated Proof of Stake	EOS, Lisk, Nano, Steem, BitShares, Ark, GXChain	
POW/POS Hybrid	IOTA, Ethereum, Dash, Power Ledger, Enigma, Dragonchain	
Federated Byzantine Agreement	Ripple, Stellar	
Byzantine Fault Tolerance	Ontology,	
Delegated Byzantine Fault Tolerance	NEO, Gas	
Practical Byzantine Fault Tolerance	Hyperledger	
Proof of Asset	DigixDao	
Proof of Storage	Siacoin	
Proof of Intelligence	Alon	
Proof of Believability	IOStoken	
Proof of Devotion	Nebulas	
Proof of Retrievability	Storj	
Proof of Authority	VeChain	

Source: White Papers, Incrementum AG

Aucune de ces stratégies n'est parfaite. Toutes correspondent à un arbitrage des développeurs entre deux tendances opposées : la centralisation de la prise de décision et son efficacité.

Comme l'expliquent H&V :

« Plus le processus décisionnel est centralisé, plus la décision peut être prise rapidement et plus le réseau est évolutif. En revanche, moins un réseau est centralisé, plus il faut de temps pour parvenir à un consensus. Ce n'est pas différent de la dichotomie entre les dictatures et les démocraties directes. »

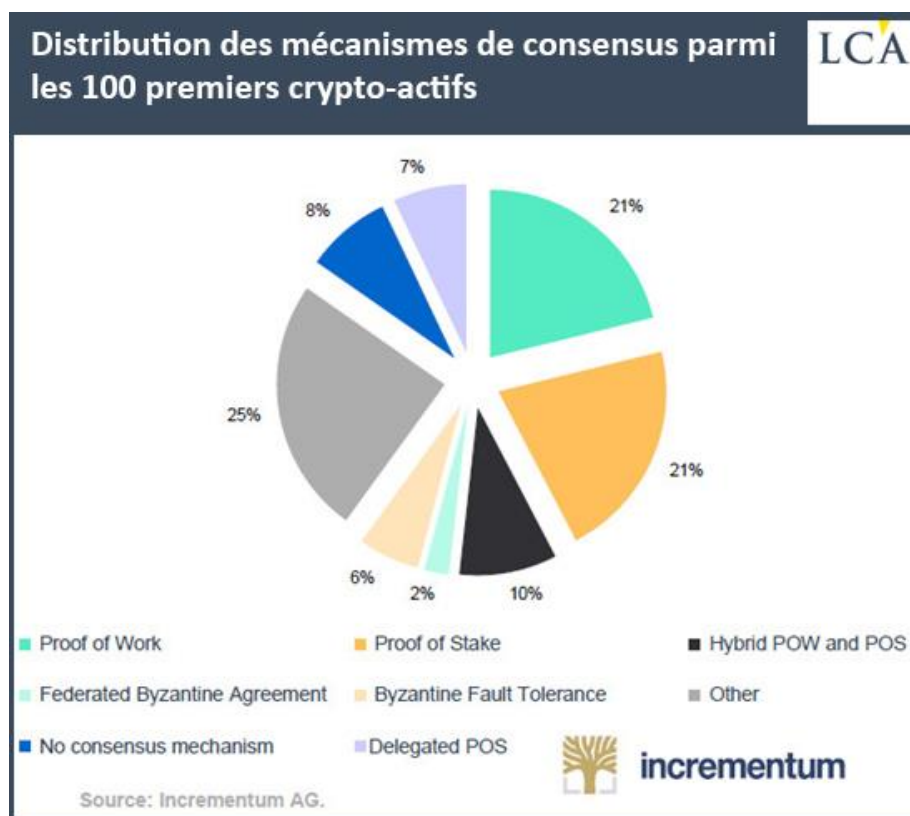
Voilà qui explique pourquoi les transactions sur le réseau Bitcoin (sept par seconde) soient aujourd'hui plus lentes que sur le réseau Visa (56 000 tps).

Qu'est-ce que ces considérations ont à voir avec la diversification de votre portefeuille de cryptos, vous demandez-vous peut-être. Il n'existe aujourd'hui pas de couverture ou *hedge* contre un marché baissier au sein des crypto-actifs. Lorsqu'elles baissent, elles le font toutes à l'unisson.

Cependant, le fait de diversifier votre portefeuille en prenant position sur des cryptos qui ne sont pas créées par des *pools* de mineurs – comme c'est typiquement le cas des actifs recourant à la POW ou « preuve de travail », beaucoup plus gourmande en ressources que ne l'est par exemple la POS, « preuve de participation » – vous prémunira d'un aléa lié à des considérations politiques.

Comme l'expliquent les auteurs du rapport :

« Les gouvernements peuvent sévir contre l'utilisation de l'électricité pour l'exploitation de crypto-monnaies, par conséquent, nous recommandons de tenir une gamme de crypto-actifs recourant à différents mécanismes de consensus ».



Diversifiez en fonction du type de registre distribué

Une autre perspective de diversification de votre portefeuille de cryptos est celle de la technologie derrière le réseau. Un autre poncif voudrait que chaque crypto-actif repose sur une blockchain, ce qui est on ne peut plus faux.

Le type de technologies dont il est question est celle des registres distribués (*distributed ledger technologies* – DLT). Elle se décompose cependant en plusieurs catégories.

La chaîne de blocs en est la plus connue, mais il existe également celle des graphes orientés acycliques (*directed acyclic graph* – DAG, comme par exemple les Tangles, ces enchevêtrements de transactions, ou encore le Hashgraph) sur laquelle reposent par exemple les protocoles IOTA, Nano et Hashgraph.

H&V décrivent ces cryptos comme des « concepts post-blockchain », en cela qu'ils pourraient résoudre le triangle d'incompatibilité des cryptos entre décentralisation, sécurité et extension avant que n'y parviennent les protocoles reposant sur la blockchain.

La première étape à franchir consiste à résoudre le problème de la rapidité du traitement des transactions, comme ces différents projets le promettent au public.

Comme vous pouvez le constater, les crypto-actifs sont loin de tous être des clones du bitcoin. Même si la monnaie-mère est aujourd'hui la plus robuste, rien n'assure qu'elle fasse partie des vainqueurs de la compétition des crypto-actifs.

Une chose est sûre, cependant : le grand ménage à venir sur les cryptos est indispensable en vue de l'arrivée de nouveaux très gros acteurs sur le marché.

Le terrain doit devenir praticable pour les institutionnels

Outre le massacre qui se prépare vis-à-vis des cryptos sans valeur intrinsèque, H&V notent deux tendances qui ont caractérisé ce premier semestre.

La première – et la plus importante de l'année pour les auteurs du rapport – est l'arrivée des grandes banques d'investissement sur le marché, ce qui a pour effet de lui apporter de la croissance et de la légitimité. C'est ce que les auteurs appellent l'« effet Goldman ».

Ces grandes banques ne considèrent plus le Bitcoin comme une « arnaque », elles développent au contraire de nouveaux *trading desks* dédiés aux crypto-actifs, comme c'est le cas de Goldman-Sachs et de J.P. Morgan. Reuters a indiqué en avril « qu'un cinquième des grandes banques veulent être en mesure de négocier des bitcoins d'ici fin 2018. »

Ce phénomène a été rendu possible par le développement des contrats à terme ou *futures* et d'autres produits dérivés du bitcoin. Depuis leur lancement en décembre 2017, les *futures* du CME ont vu leur volume de trading quotidien progresser de 250%.

La seconde tendance découle de la première :

« Les régulateurs se trouvent de plus en plus sous pression car les investisseurs institutionnels ont besoin de sécurité juridique avant de pouvoir entrer sur le marché. »

Cette perspective a donné lieu aux premiers resserrements de la réglementation décidés par la SEC.

H&V rappellent qu'« à l'heure actuelle, il est toujours interdit aux investisseurs institutionnels d'acheter du bitcoin en dehors des fonds réglementés, des trackers, des contrats à terme et des *trusts*. »

Les investisseurs institutionnels « se préparent cependant pour le jour où cela sera possible, et ils réfléchissent sérieusement à des moyens d'acheter directement des bitcoins et de les stocker en toute sécurité pour les clients. »

Que retenir de tout cela pour vos investissements ?

Bitcoin est désormais devenu « grand public », estiment H&V. Les cryptomonnaies sont là pour rester même si... on ignore évidemment lesquelles survivront.

Compte tenu de la très faible capitalisation des cryptos en comparaison des autres classes d'actifs, on est en droit d'espérer que sur le long terme, les cryptos représentent une opportunité de gain considérable. [NDLR : Mettez maintenant en portefeuille ces cryptomonnaies de « 3ème génération » – celles qui ont les meilleures chances de percer sur le marché, aux côtés du bitcoin. [Découvrez-les ici.](#)]

Si vous êtes déjà positionné sur le marché, il semble trop tôt pour renforcer vos positions. Si vous êtes en dehors et que vous êtes pris d'une irrépressible peur de rater le train des cryptos, sachez que vous y rentrerez à vos risques et périls et que vous pourriez bien voir la vallée de la mort d'assez près pendant votre voyage.

Une position intermédiaire, souvent la plus sage pour l'investisseur peu aguerri, consiste à mettre en place des ordres d'achat programmés à intervalles réguliers sur votre plateforme d'échange, de manière à lisser votre prix d'achat moyen.

Il n'est cependant pas trop tard pour développer votre connaissance de ces technologies dont certaines d'entre elles promettent rien de moins que de changer la monnaie, donc le monde des échanges.