

CLASSE : Protocoles de consensus [Blockchain]

1. algebraic holographic protocol (AHP) [protocole holographique algébrique (PHA)]
2. (blockchain) consensus protocol; consensus algorithm; validation mechanism [protocole de consensus ; algorithme de consensus ; mécanisme de validation]
3. Byzantine Fault Tolerance protocol; BFT protocol (protocole de tolérance des Byzantins ; protocole BFT)
4. delegated proof of stake (DPoS) [preuve d'enjeu déléguée (DPoS)]
5. liquid proof of stake (LPoS) [preuve d'enjeu liquide (LPoS)]
6. Nakamoto protocol (protocole de Nakamoto)
7. nominated proof of stake (NPoS) [preuve d'enjeu nominée (NPoS)]
8. proof-of-authority (PoA) [preuve d'autorité (PoA)]
9. proof-of-burn (preuve de destruction ; preuve de réputation)
10. proof of elapsed time (PoET) [preuve du temps écoulé (PoET)]
11. proof-of-hold (preuve de possession)
12. proof of useful work (PoUW) [preuve de travail utile (PoUW)]
13. Snow protocol; Snow consensus protocol (protocole de consensus de Snow ; protocole de Snow)
14. ticketed proof of stake (TPoS) [preuve d'enjeu étiquetée (TPoS)]

ALGEBRAIC HOLOGRAPHIC PROTOCOL (AHP), N. 'consensus protocol...'		PROTOCOLE HOLOGRAPHIQUE ALGÈBRIQUE (PHA), N. masc. 'protocole de consensus'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
Consensus protocol that obliges the transaction prover to send not only an implicit proof but also a low-degree polynomial oracle to the verifier, who encodes it holographically and validates the transaction much faster.		Protocole de consensus qui oblige le prouveur d'une transaction d'envoyer, en plus d'une preuve implicite, un oracle en polynômes de faible degré au vérificateur qui le code holographiquement et valide la transaction bien plus rapidement.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Realization verb	to rely [on ART ~] to scale [ART ~]	Verbe de réalisation	se fier [à ART ~] mettre [ART ~] à l'échelle
Context		Contexte	
<i>Algebraic holographic proofs</i> (AHPs) modify the notion of an IOP by enabling the verifier not to receive its input explicitly but, rather, to have access to and encode the oracle sent by the prover (holographic change); and by ensuring that the honest prover must produce oracles that are low-degree polynomials (this restricts the completeness property). [Chiesa et al. 2021]		La robustesse des preuves de consensus a aussi recours à l'oracle en tant que source d'informations fiables ; par exemple, les PHA (preuves holographiques algébriques) impliquent des oracles pour renforcer la qualité des informations fournies aux vérificateurs. [Martin 2019]	

(BLOCKCHAIN) CONSENSUS PROTOCOL , N. 'consensus protocol'		PROTOCOLE DE CONSENSUS (DE BLOCKCHAIN) , N. masc. 'protocole de consensus'	
Variant		Variante	
Synonym		Synonyme	
CONSENSUS ALGORITHM; VALIDATION MECHANISM		ALGORITHME DE CONSENSUS ; MÉCANISME DE VALIDATION	
Definition		Définition	
Mechanism that defines how the users of a blockchain should reach an agreement for the validation of transactions.		Mécanisme qui détermine le mode de réalisation de consensus entre les utilisateurs d'une blockchain en vue de la validation de transactions.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Types of consensus protocols	Byzantine fault tolerance (BFT) protocol Byzantine fault tolerance proof delegated proof of stake (BFT-DPoS) delegated proof-of-stake (DPoS) liquid proof of stake (LPoS) mutualized proof of stake (MPoS) Nakamoto protocol nominated proof of stake (NPoS) proof-of-authority (PoA) proof-of-burn proof of contribution (PoC) proof-of-hold proof-of-importance (PoI) proof of reserve (PoR) proof-of-space proof-of-stake (PoS) proof of time elapsed (PoET) proof-of-use proof-of-useful work (PouW) proof-of-work (PoW) Snow protocol ticketed proof of stake (TPoS)	Types de protocole de consensus	protocole de tolérance des Byzantins preuve d'enjeu déléguée à tolérance des Byzantins (BFT-DPoS) preuve d'enjeu déléguée (DPoS) preuve d'enjeu liquide (LPoS) preuve d'enjeu mutualisée (MPoS) protocole de Nakamoto preuve d'enjeu nominée (NPoS) preuve d'autorité (PoA) preuve de destruction (= preuve de réputation) preuve de contribution (PoC) preuve de possession preuve d'importance preuve de réserves (PoR) preuve de capacité preuve d'enjeu (PoS) [≠ preuve de participation] preuve du temps écoulé (PoET) preuve d'utilisation preuve de travail utile preuve de travail (PoW) protocole de Snow preuve d'enjeu étiqueté (TPoS)
	distributed consensus protocol		protocole de consensus distribué
Context		Contexte	
Blockchain consensus protocols are the key piece of the puzzle in the blockchain's operating model, [...] as they decide how the agreement should be reached among miners to append a new block to the chain. [Moudoud 2022]		Les protocoles de consensus qui sont au cœur des blockchains publiques reposent tous sur des mécanismes d'incitation économique qui requièrent l'émission d'un actif numérique. [France Stratégie 2018]	

PROOF OF AUTHORITY, N. 'consensus protocol...'	PREUVE D'AUTORITÉ, N. fém. 'protocole de consensus'
Variant	Variante
Synonym	Synonyme
Definition	Définition
Permission-based consensus protocol that empowers some blockchain users to serve as transaction validators and/or managers.	Protocole de consensus de blockchain fermée qui habilite certains utilisateurs de la chaîne à jouer le rôle de validateurs et/ou de gestionnaires de transactions.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
Instead of working or staking coins to prove its right to create a block, the proof-of-authority (PoA) simply gives the right to certain nodes (called sealers or validators) in the network to create blocks. [Djari 2023]	La preuve d'autorité (PoA) est propre aux protocoles privés : il s'agit du mode de consensus le plus simple, puisqu'une autorité centrale attribue le droit de miner un bloc selon des modalités définies par elle. [Faure-Muntian et al. 2018]

BYZANTINE FAULT TOLERANCE (BFT) PROTOCOL , N. 'consensus protocol'		PROTOCOLE DE TOLÉRANCE DES BYZANTINS , N. masc. 'protocole de consensus'	
Variant		Variante	
Synonym		Synonyme	
BFT PROTOCOL		PROTOCOLE BFT ; PROTOCOLE DE TOLÉRANCE DES FAUTES BYZANTINES	
Definition		Définition	
Consensus protocol based on a blockchain network's ability to reach consensus and keep operating in spite of the deficiency of some of its nodes.		Protocole de consensus basé sur la capacité d'une blockchain à atteindre le consensus et à continuer à fonctionner malgré la défaillance de certains de ses nœuds.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Generic term	(blockchain) consensus protocol	Terme générique	protocole de consensus (de blockchain)
Types of BFT protocols	asynchronous Byzantine fault tolerance (aBFT) protocol delegated Byzantine fault tolerance (dBFT) protocol fast Byzantine fault tolerance (fBFT) protocol multi-level Byzantine fault tolerance protocol practical Byzantine fault tolerance (pBFT) protocol	Types de protocoles BFT	protocole de tolérance des byzantins asynchrone (aBFT) protocole de tolérance des byzantins délégué (dBFT) protocole de tolérance des byzantins rapide (fBFT) protocole de tolérance des byzantins multi-échelles protocole de tolérance des byzantins pratique (pBFT)
Note		Note	
Byzantine node		nœud byzantin [nœud blockchain corrompu à la suite d'une attaque/faute byzantine]	
Context		Contexte	
The Byzantine Fault Tolerance (BFT) protocols adopted by Bitcoin allow for a probabilistic safety guarantee and for assuming honest majority computational power rather than a known membership, which in turn has enabled the internet-scale permissionless protocol. [Rocket et al. 2020]		Les validateurs de la blockchain exécutent le protocole de consensus de <i>tolérance des byzantins (BFT)</i> à chaque tour i pour finaliser le i ème bloc, ce après quoi un nouveau consensus BFT est exécuté pour finaliser le bloc $i + 1$, et ainsi de suite. [Axelar 2021]	

DELEGATED PROOF OF STAKE (DPoS), N. 'consensus protocol'	PREUVE D'ENJEU DÉLÉGUÉE (DPoS), N. fém. 'protocole de consensus'
Variant	Variante
Synonym	Synonyme
Definition	Définition
Consensus protocol derived from PoS that allows blockchain users to delegate their own stake to their elected validator and share the block reward with him.	Protocole de consensus dérivé de la PoS qui permet à l'utilisateur de la blockchain de déléguer ses actifs au validateur choisi et partager avec lui la prime de transaction.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
With the Delegated Proof-of-Stake (DPoS) protocol, token holders can delegate part of their staked assets to validators who have a better chance of being selected. [Djari 2022]	La blockchain Axelar suit un modèle de preuve d'enjeu déléguée (DPoS) similaire à celui de Cosmos Hub : les utilisateurs élisent des validateurs qui doivent bloquer leur enjeu pour participer au consensus et maintenir un service de haute qualité. [Axelar 2021]

LIQUID PROOF OF STAKE (LPoS), N. 'consensus protocol'	PREUVE D'ENJEU LIQUIDE (LPoS), N. fém. 'protocole de consensus'
Variant	Variante
Synonym	Synonyme
Definition	Définition
Consensus protocol derived from PoS that allows blockchain users to directly exercise their voting rights or transfer them to an elected delegate while keeping their assets.	Protocole de consensus dérivé de la PoS qui permet aux utilisateurs d'une blockchain de voter directement ou d'en transférer les droits à un délégué choisi, mais de conserver leurs actifs.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
The Liquid Proof-of-Stake (LPoS) consensus, which came up in the wake of liquid democracy, allows asset owners to delegate their voting rights without transferring their funds to a given validation node. [Djari 2022]	La preuve d'enjeu liquide (LPoS) suit le principe de démocratie liquide portée par la révolution blockchain : le citoyen peut faire le choix, soit de voter directement pour le décideur, soit de déléguer son autorité démocratique à un représentant, chargé d'élire le décideur. [Rodriguez 2017]

NAKAMOTO (CONSENSUS) PROTOCOL, N. 'consensus protocol'		PROTOCOLE (DE CONSENSUS) DE NAKAMOTO, N. masc. 'protocole de consensus'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
Consensus protocol of Bitcoin's first version, which aimed to be highly decentralized, public, and robust through asymmetric algorithms and hash functions.		Protocole de consensus de la première version de Bitcoin, qui se voulait fortement décentralisée, publique et robuste grâce à des algorithmes asymétriques et des fonctions de hachage.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Realization verb	to implement [ART ~] to use [ART ~]	Verbe de réalisation	implémenter [ART ~] utiliser [ART ~]
Note		Note	
Nakamoto consensus protocols are generally assimilated to PoW protocol models. By contrast, any PoS or mixed consensus protocols that apply the Nakamoto principles are called " Nakamoto-like protocols ".			
Context		Contexte	
Nakamoto consensus protocols have become popular with the rise of Bitcoin, providing a probabilistic safety guarantee: Nakamoto consensus decisions may revert with some probability <i>e</i> . [Rocket et al. 2020]		Le protocole de Nakamoto se fonde sur deux outils cryptographiques : la signature électronique à clé publique fondée sur des algorithmes asymétriques et les algorithmes de hachage, tous deux étant sont des fonctions à sens unique. [Faure-Muntian et al. 2018]	

NOMINATED PROOF OF STAKE (NPoS), N. 'consensus protocol'	PREUVE D'ENJEU NOMINÉE (NPoS), N. fém. 'protocole de consensus'
Variant	Variante
Synonym	Synonyme
Definition	Définition
Consensus protocol that allows blockchains to have a first set of validators called nominators, who in turn choose their trusted validator nodes for staking and validation.	Protocole de consensus qui permet aux blockchains de disposer d'un premier groupe de validateurs appelés nominateurs, qui, à leur tour, choisissent leurs nœuds de jalonnement et de validation des transactions.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
First implemented by Polkadot, the Nominated Proof of Stake (NPoS) separates the roles of staking and validation: to participate in the block-update process, the validators are elected by the so-called nominators, who only commit their assets to trusted validators who able to maximize their staking returns. [Oderbolz et al. 2023]	La preuve d'enjeu nominée (Nominated Proof of Stake, NPoS) est une variation de la preuve d'enjeu (PoS) qui permet aux détenteurs de jetons de participer au processus de validation des transactions et de sécurisation du réseau en choisissant des nœuds de confiance qui seront responsables de la validation des transactions. [Gaouaou 2023]

PROOF-OF-BURN, N. 'consensus protocol'	PREUVE DE DESTRUCTION, N. masc. 'protocole de consensus'
Variant	Variante
PROOF OF BURN	
Synonym	Synonyme
	PREUVE DE RÉPUTATION. PREUVE DE BRÛLAGE [impropre]
Definition	Définition
Consensus protocol derived from the proof-of-stake which compels miners to dispose of crypto-assets to gain the network's evidence.	Protocole de consensus dérivé de la preuve d'enjeu qui oblige le mineur à supprimer des cryptoactifs afin de gagner la confiance du réseau.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
In Proof-of-Burn (PoB), a potential miner has to burn coins, which however need to be generated in order to be burnt, thus the need for another way to create blocks. [Djari 2023]	La preuve de destruction représente l'obligation pour les mineurs de détruire des cryptoactifs pour obtenir la confiance du réseau. [Faure-Muntian et al. 2018]

PROOF OF ELAPSED TIME (PoET), N.		PREUVE DU TEMPS ÉCOULÉ (PoET), N.	
'blockchain protocol'		masc. 'type de protocole de consensus'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
Consensus protocol based on a random amount of waiting time each node must observe before broadcasting a block for validation.		Protocole de consensus basé sur un temps d'attente aléatoire que chaque nœud de la blockchain doit observer avant de soumettre un bloc pour validation.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Realization verb	to serve [as ART ~]	Verbe de réalisation	servir [de ART ~]
Context		Contexte	
In a blockchain using a proof of Elapsed Time, the validator with the shortest waiting time for a transaction block is elected as the leader, and the distribution of elected leaders across the entire population of validators is similar to what is provided by other lottery algorithms. [Lee Kuo and Low 2021]		Le protocole de consensus pour Sawtooth Lake s'appelle la preuve du temps écoulé (PoET) ; il a été construit pour fonctionner dans un environnement de l'exécution approuvé (TEE) sécurisé [...] et prouver que le temps s'est écoulé via des transactions horodatées. [Laurence 2018]	

PROOF-OF-HOLD, N. 'blockchain protocol'	PREUVE DE POSSESSION, N. fém. 'protocole de consensus'
Variant	Variante
PROOF OF HOLD	
Synonym	Synonyme
PROOF OF POSSESSION; PROOF OF HOLDING MECHANISM	
Definition	Définition
Consensus protocol derived from the proof-of-stake that compels blockchain users to prove that they hold a certain amount of crypto-assets for a defined period before allowing them to make transactions.	Protocole de consensus dérivé de la preuve d'enjeu, qui oblige les utilisateurs de la blockchain à prouver qu'ils détiennent un certain volume de cryptoactifs pour un temps déterminé avant d'être autorisés à effectuer des transactions.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
The proof-of-hold (PoH), or proof of holdings mechanism, is based on the fact of having held your assets for a minimum time (minimum holding time). [Galeon 2024]	La preuve de possession consiste en une signature électronique de la transaction précédente, [étant que] de transaction en transaction, il est possible de remonter à l'origine de la création du satoshi et donc de vérifier qu'il n'y a pas de double dépense. [Faure-Muntian et al. 2018]

PROOF OF USEFUL WORK (PoNW), N.	PREUVE DE TRAVAIL UTILE (PoNW), N.
‘blockchain protocol’	fém. ‘protocole de consensus’
Variant	Variante
Near Synonym	Synonyme approximatif
proof of useful work (PoUW)	preuve de travail nécessaire
Definition	Définition
Consensus protocol stemming from PoW that generates succinct zk-proofs of validity and thus improve the system’s verification and security during the user’s efforts.	Protocole de consensus dérivé de PoW qui génère de brèves preuves de validité ZK et améliore ainsi le travail de vérification et de sécurité du système lors des efforts de l’utilisateur.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
The Proof of Useful Work (PoUW), introduced by Kattis and Bonneau, offers a blockchain’s Sybil resistance mechanism, [...] ensuring that the computational efforts dedicated to Sybil resistance also contribute to the system’s verification. [Motepalli et al. 2023]	La preuve de travail utile est une modification de la preuve de afin de rendre utile la phase de minage, et pour ce faire, la condition que le mineur est censé vérifier en trouvant un bloc avec son hash devient modifiable. [Martin 2019]

SNOW PROTOCOL, N. 'blockchain protocol'	PROTOCOLE DE SNOW, N. masc. 'protocole de consensus'
Variant	Variante
Near Synonym	Synonyme approximatif
Definition	Définition
Consensus protocol based on a system that samples repeatedly the network at random, steering correct nodes towards a common outcome to provide a probabilistic safety guarantee against consensus failure.	Protocole de consensus basé sur un système qui échantillonne itérativement de manière aléatoire, en dirigeant les nœuds non corrompus vers un résultat commun afin d'apporter une garantie de sécurité probabiliste contre des échecs de consensus.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
Inspired by gossip algorithms, Snow protocols are a new family of consensus mechanisms that gains its properties through a system that operates by repeatedly sampling the network at random, steering correct nodes towards a common outcome. [Rocket et al. 2020]	Inspiré par des algorithmes de rumeur, les protocoles de Snow constituent une nouvelle famille de mécanismes de consensus qui acquiert ses propriétés à travers un système qui opère par échantillonnage itératif et aléatoire du réseau, et en dirigeant les nœuds non corrompus vers un résultat commun. [Rocket et al. 2020, traduction]

TICKETED PROOF OF STAKE (TPoS), N. 'blockchain protocol'	PREUVE D'ENJEU ÉTIQUETÉE (TPoS), N. fém. 'protocole de consensus'
Variant	Variante
Synonym	Synonyme
Definition	Définition
Consensus protocol that obliges miners to buy tickets to be allowed to add blocks to the chain.	Protocole de consensus qui oblige les mineurs à acheter des tickets avant d'être autorisés à ajouter des blocs à la chaîne.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Context	Contexte
Fusion represents a permutation on a PoS network with token rewards based on participating in staking via a Ticketed Proof of Stake (TPoS) consensus mechanism, which involves buying tickets to potentially be given the right to generate the next block. [Jincheng et al. 2023]	Contrairement à la preuve du temps écoulé (PoET), qui évalue le temps mis sur un réseau dans l'intention d'effectuer une transaction (en l'occurrence un jalonnement), la preuve d'enjeu étiquetée (TPoS) soumet toute participation dans le réseau à l'obtention de tickets. [Cryptomus 2024]