CLASSE : Verrous cryptographiques [Blockchain]

1. hash1 (empreinte cryptographique ; empreinte numérique ; hache)
2. hash2 ; hashing ; hash coding (hachage)
3. elliptic curve digital signature algorithm (ECDSA) [algorithme de signature numérique à courbes elliptiques (ECDSA) ; algorithme ECDSA]
4. hash [to] (hacher)
5. Hash-based Message Authentication Code (HMAC) [code d'authentification de message par hachage (HMAC)]
6. hash puzzle; cryptographic puzzle (opération cryptographique de hachage)
7. hash time locked contract (HTLC) [contrat à verrou cryptographique temporel ; contrat HTCL)]
8. nonce ; nonce value (nonce ; valeur nonce)
9. point time locked contract (PTLC) [contrat à points de verrouillage (PTLC)]
10. revocable sequence maturity contract (RSMC) [contrat intelligent révocable à échéance (RSMC)]

AUTOMATED MARKET MARKER (AMM), N. 'cryptographic lock'		**TENEUR DE MARCHÉ AUTOMATISÉ (AMM)**, N. masc. 'verrou cryptographique'	
Variant		Variante	
		TENEUR DE MARCHÉ AUTOMATISÉ	
Synonym		Synonyme	
AMM PROTOCOL		PROTOCOLE AMM	
Definition		Définition	
Cryptographic lock that ensures decentralized exchanges of crypto assets on blockchain platforms are automated and do not need authorization.		Verrou cryptographique qui veille à l'automatisation des échanges décentralisés de cryptoactifs sur des plateformes et à la non-nécessité d'une autorisation.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Cooccurrence		Cooccurrence lexicale	
Types of AMM	concentrated liquidity AMM (CLAMM) synthetic AMM (sAMM) dark-pool [~] private [~] public [~]	Types d'AMM	AMM de liquidités concentrées (CLAMM) AMM synthétisé (sAMM) [~] sans pool officiel [~] privé [~] public
Realization verb	to centralize [ART ~] to sophisticate [ART ~] to build [on ART ~]	Verbe de réalisation	centraliser [ART ~] moderniser [ART ~] ; sophistiquer [ART ~] s'appuyer [sur ART ~]
Frequent Expressions		Expressions fréquentes	
[~] system [~]'s gamma [~]'s liquidity pool [~]'s trading function dark [~]'s pool to inflate asset prices [on ART ~]		système [de ART ~] gamma [de ART ~] pool de liquidités [de ART ~] fonction d'échange [de ART ~] pool non officiel [de ART ~] faire monter les prix des actifs [sur ART ~]	
Context		Contexte	
With a lower entry barrier, Automated Market Makers (AMMs) have achieved their prevalence in the DeFi space, which enables the market maker to act as an LP [liquidity provider] and to deposit only two or multiple different tokens to the liquidity pool. [Fouda 2023]		Osmosis, le teneur de marché automatisé (AMM) basé à Cosmos, utilise la mission d'interconnectivité en un clic pour concrétiser sa vision d'un internet des blockchains. [Axelar Franco 2023]	

(CRYPTOGRAPHIC) HASH, N. 'cryptographic lock'		**EMPREINTE CRYPTOGRAPHIQUE,** N. fém. 'verrou cryptographique'	
Variant		Variante	
HASH			
Synonym		Synonyme	
DIGITAL FINGERPRINT; HASH CODE; ROOT HASH		EMPREINTE NUMÉRIQUE ; HACHE (N. masc.) ; IDENTIFIANT CRYPTOGRAPHIQUE	
Near Synonym		Synonyme approximatif	
HASH VALUE		VALEUR DE HACHAGE ; CONDENSÉ	
Definition		Définition	
Cryptographic lock created during the production of a transaction block or a file to serve as their unique, timestamped, and tamper-proof identifier.		Verrou cryptographique créée lors de la production d'un bloc de transaction ou d'un fichier pour leur servir d'identifiant unique, horodatée et infalsifiable.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
The cryptographic hash of a transaction block **[*of* ART *N*]** A block's hash **[*N's*]**		L'empreinte cryptographique d'un bloc de transaction **[*de* ART *N*]**	
Lexical Cooccurrence		Cooccurrence lexicale	
Hash of what	(transaction) block; data file; document; key; rollup; text; transaction	Empreinte cryptographique de quoi	bloc (de transaction); fichier de données ; document; clé ; rollup; texte ; transaction
Antonym	To de-hash	Antonyme	déhacher[rare]
Potential adjective	(that can be hashed)	Adjectif potentiel	hachable
Nominalization	hashing (= hash coding)	Nominalisation	hachage
Realization verb	to assign [ART ~] to check [ART ~] to compute [ART ~] to generate [ART ~] to integrate [ART ~] to register [ART ~] to validate [ART ~]	Verbe de réalisation	attribuer [ART ~] vérifier [ART ~] calculer [ART ~] générer [ART ~] intégrer [ART ~] enregistrer [ART ~] ; sauvegarder [ART ~] valider [ART ~]
Frequent Expressions		Expressions fréquentes	
[~] algorithm [~] -Based Message Authentication Code (HMAC) [~] bucket [~] computation [~] function [~] iterative framework (HAIFA) [~] length		algorithme de hachage code d'authentification de message par hachage (HMAC) panier [de ART ~] calcul [de ART ~] fonction [de ART ~] cadre itératif de hachage (HAIFA) longueur de l'[ART ~]	

[~] per second (H/S) [~] power [~] puzzle [~] rate [~] table [~] time Cashhash double [~] Equihash Ethash Full Domain [~] (FDH) signature hashgraph hashlock key hashmask Merkle root [~] SHA-256 [~] algorithm	~ par seconde puissance de hachage (= puissance de calcul [de hachage]) équation cryptographique taux de hachage table de hachage durée de hachage Cashhash double ~ Equihash Ethash signature cryptographique domaine global (= signature FDH) graphe de haches (= graphe-hash) clé à verrouillage par hachage (= verrou cryptographique) jeton à masque [~] de la racine de Merkle algorithme de hachage SHA-256
Context	Contexte
The cryptographic hash of a block or a data file is like a signature for that block or data file, generated as an almost-unique, fixed size 256-bit (32-byte) code that cannot be decrypted back. [Lee Kuo and Low 2018]	La blockchain peut ainsi servir de registre certifiant, pour enregistrer l'empreinte cryptographique (hash) d'un document (un acte notarié par exemple) et permettre ainsi de prouver l'existence d'un document à un moment T. [Faure-Muntian et al. 2018]

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA), N. 'cryptographic lock'		**ALGORITHME DE SIGNATURE NUMÉRIQUE A COURBES ELLIPTIQUES (ECDSA)**, N. masc. 'verrou cryptographique'	
Variant		Variante	
		ALGORITHME ECDSA	
Synonym		Synonyme	
Definition		Définition	
Cryptographic lock based on signature inalterability that is used to secure blockchain data and funds and enable transfer to their rightful owners.		Verrou cryptographique fondé sur l'infalsifiabilité des signatures qui permet de sécuriser les données et les fonds des blockchains ainsi que leur transfert aux ayants droit.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Cooccurrence		Cooccurrence lexicale	
Type of ECDSA	Edwards-curve Digital Signature Algorithm (EdDSA)	Type d'ECDSA	Algorithme de signature numérique à courbes d'Edward (EdDSA)
Realization verb	to develop [ART ~] to use [ART ~]	Verbe de réalisation	développer [ART ~] utiliser [ART ~]
Context		Contexte	
Elliptic Curve Digital Signature Algorithm or ECDSA is a cryptographic algorithm to "sign" an array in a special way so that third parties can easily verify the authenticity of the signature, but the signer reserves the exclusive ability to create signatures. [Prasaath 2023]		Un verrou permet de produire une seconde clé appelée clé publique : pour le bitcoin, il s'agit d'un algorithme de signature numérique à courbes elliptiques, appelé ECDSA. [Faure-Muntian *et al.* 2018]	

HASH [TO], tr. V. 'cryptographic lock'		**HACHER,** V. tr. 'verrou cryptographique'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
To create the cryptographic hash of a bloc or file.		Créer l'empreinte cryptographique d'un bloc ou d'un fichier.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
The miner **[*N*]** hashes the blocks **[ART *N*]** using the supercomputer's computing power.		Les nœuds de Bitcoin **[*N*]** ne hachent pas de l'ether **[*de* ART $N_{<cryptomonnaie>}$]**.	
Lexical Cooccurrence		Cooccurrence lexicale	
Who/what hashes	blockchain; hash function (= hash algorithm); (blockchain) node; system; validator	Qui/ce qui hache	Blockchain ; fonction de hachage ; nœud (blockchain) ; système ; validateur
What is hashed	(transaction) block; block header; data file; data	Ce qui est haché	bloc (de transaction) ; en-tête de bloc ; fichier de données ; données
Antonym	to unhash (= to de-hash)	Antonyme	déhacher
Nominalization	hashing (= hash coding)	Nominalisation	hachage
Context		Contexte	
For a miner to successfully mine and get the bitcoin reward, there is a need for another Bitcoin node to hash the block. By doing this, you provide a summary of the data contained in a particular block. [Yang et al. 2022]		La blockchain Factom prend le jeu de données complet et le hache jusqu'à ce qu'il n'y ait plus qu'un seul hash qui puisse représenter l'ensemble de la blockchain. [Laurence 2018]	

HASH PUZZLE, N. 'cryptographic lock'		**ÉPREUVE CRYPTOGRAPHIQUE**, N. fém. 'verrou cryptographique'	
Variant		Variante	
Synonym		Synonyme	
CRYPTOGRAPHIC PUZZLE		ÉQUATION CRYPTOGRAPHIQUE ; OPÉRATION CRYPTOGRAPHIQUE	
Quasi-synonym		Synonyme approximatif	
CRYPTOGRAPHIC HASHING		HACHAGE CRYPTOGRAPHIQUE ; MINAGE	
Definition		Définition	
Mathematical operation that a miner proof-of-work blockchains must solve in a competition with peers in order to get the block validated and gain a reward.		Équation mathématique qu'un mineur de blockchain à preuve de travail doit résoudre, dans une compétition avec ses pairs, afin de faire valider le bloc et recevoir une prime.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Cooccurrence		Cooccurrence lexicale	
Generic term	security mechanism	Terme générique	verrou cryptographique
Realization verb	to deal with [ART ~] to solve [ART ~]	Verbe de réalisation	affronter une [ART ~] résoudre une [ART ~]
Context		Contexte	
The miner who first solves the hash puzzle is allowed to broadcast his block on the peer-to-peer network; the block also includes the solution to the puzzle, also called the nonce, in the block header. [Soze 2017]		Les mineurs (membres de la communauté mettant à disposition leur puissance de calcul) doivent résoudre une véritable épreuve cryptographique qui consiste à trouver la valeur de la « preuve de travail » (ou Proof of Work) permettant de valider le bloc. [Bajolle et Godé 2021]	

HASH TIME LOCKED CONTRACT (HTLC), N. 'cryptographic lock'		**CONTRAT À VERROU CRYPTOGRAPHIQUE TEMPOREL (HTLC),** N. masc. 'verrou cryptographique'	
Variant		Variante	
HASHED TIMELOCK CONTRACT			
Synonym		Synonyme	
		CONTRAT HTLC ; CONTRAT À CLE CRYPTOGRAPHIQUE	
Definition		Définition	
Cryptographic lock that secures a transaction with a hash and requires the recipient to unlock it with a pre-image and provide a cryptographic proof of payment within a specified time frame in order to claim the funds.		Verrou cryptographique qui sécurise une transaction par hachage qui permet au destinataire de la déverrouiller avec une pré-image et de soumettre une preuve cryptographique de versement dans un délai précis afin de réclamer les fonds.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Cooccurrence		Cooccurrence lexicale	
Realization verb	to distinguish between [ART ~ and N]	Verbe de realization	distinguer le [ART ~ de N]
Frequent Expressions		Expressions fréquentes	
HTLC-based payment channel attack [against ART ~]		canal de paiement par HTLC attaque [contre ART ~]	
Context		Contexte	
A Hash Time Locked Contract (HTLC) is a smart contract that requires the recipient to provide a cryptographic proof of payment within a specified time frame, in order to claim the funds; if the recipient fails to provide this proof, the funds will be returned to the sender. [Jincheng et al. 2023]		Le contrat à verrou cryptographique temporel (HTLC) est une fonctionnalité des plateformes blockchain qui oblige le destinataire d'une transaction de type HTLC à accuser réception du paiement en soumettant une preuve cryptographique dans un certain délai. [Vernay 2023]	

HASH-BASED MESSAGE AUTHENTICATION CODE (HMAC), N. 'cryptographic lock'	**CODE D'AUTHENTIFICATION DE MESSAGE PAR HACHAGE (HMAC)**, N. masc. 'verrou cryptographique'
Variant	Variante
	CODE HMAC
Synonym	Synonyme
Definition	Définition
One-time password lock that is built on a cryptographic function and secret key to ensure the verification of a message's authenticity by both the sender and the receiver.	Verrou avec mot de passe à usage unique qui exploite une fonction et une clé secrète cryptographiques pour permettre à l'expéditeur et au destinataire d'un message de vérifier son authenticité.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Cooccurrence	Cooccurrence lexicale
Realization verb: to decrypt [ART ~]	Verbe de réalisation: décrypter [ART ~]
Frequent Expressions	Expressions fréquentes
HMAC key HMAC process HMAC test	clé HMAC processus HMAC test HMAC
Context	Contexte
The cryptographic function and cryptographic secret key of the Hash-Based Message Authentication Code (HMAC) are combined with the original message to create a hash in the HMAC hashing process, ensuring that both parties can verify the authenticity of the message. [Solomon 2023]	Le code d'authentification de message par hachage (HMAC) est une technique d'authentification cryptographique qui utilise une fonction de hachage et une clé secrète afin de vérifier que les données sont correctes et authentiques avec des secrets partagés. [Okta 2023]

NONCE, N. 'cryptographic lock'		**NONCE**, N. masc. 'verrou cryptographique'	
Variant		Variante	
Synonym		Synonyme	
NONCE VALUE; PoW NONCE		VALEUR NONCE	
Definition		Définition	
Additional cryptographic lock consisting of a number only used once that is added to a block hash during the mining process.		Verrou cryptographique supplémentaire sous forme de nombre à usage unique qui est ajouté à l'empreinte cryptographique d'un bloc au cours du minage.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
The nonce of a block hash **[*of* ART *N*]** A block's **[*N*'s]** nonce		Le nonce d'un hache de bloc **[*de* ART *N*]**	
Lexical Relations		Relations lexicales	
Nonce of what	block; hash; hash code	Nonce de quoi	bloc ; empreinte cryptographique (= hash)
Realization verb	to alter [ART ~]; to increment [ART ~]	Verbe de réalisation	modifier [ART ~]; incrémenter [ART ~]
Context		Contexte	
In order to avoid centralization of computing power, the nonce of next block generation is dynamically changed on the basis of 10 minutes per block. [Thien Huyinh-The et al. 2023]		Le « nonce » du hash de ce bloc correspond quelques chiffres qui sont ajoutés pour que le hash réponde à une certaine propriété, par exemple qu'il commence par un certain nombre de 0. [Faure-Muntian et al. 2018]	

PLONK, N. 'cryptographic lock'		**PLONK**, N. masc. 'verrou cryptographique'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
ZKP-SNARK-based cryptographic lock that provides a single trusted setup for all circuits and applications and is initiated once and permanently reusable.		Verrou cryptographique basé sur ZK-SNARK qui fournit une seule installation de confiance pour tous les circuits et applications et est initialisé une seule fois et indéfiniment réutilisable.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Types of PLONKs	Plonky1 Plonky2	Types de PLONKs	Plonky1 Plonky2
Adjectivation	PLONK-ish	Adjectivation	de PLONK
Realization verb	to compare [~ *with* N] to evaluate [~]	Verbe de réalisation	comparer [~ *avec* N] évaluer [~]
Context		Contexte	
The ZKP progress continued with the introduction of PLONK in 2019 which is a SNARK implementation that allows a single trusted setup to be used by many applications without repeating the setup. [Fouda and Wang 2022]		PLONK est conçu pour fournir une solution ZKP universelle et efficace, en particulier dans les applications blockchain telles que les contrats intelligents et les transactions protégées par la confidentialité ; au cœur de PLONK se trouve un verrou de « dissimulation homomorphique ». [Wayne et Pipo 2023]	

POINT TIME LOCKED CONTRACT, N. 'cryptographic lock'		**CONTRAT À POINTS DE VERROUILLAGE**, N. masc. 'verrou cryptographique'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
Smart contract that locks a transaction with a private key and requires the recipient to unlock it by providing a corresponding digital signature that reveals the hidden value.		Contrat intelligent qui verrouille une transaction à l'aide d'une clé privée et exige que le bénéficiaire la déverrouille en fournissant une signature numérique correspondante qui révèle la valeur cachée.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Cooccurrence		Cooccurrence lexicale	
Realization verb	to develop [ART ~] to transact [with ART ~] to use [ART ~]	Verbe de réalisation	mettre au point [ART ~] faire des transactions [avec ART ~] utiliser [ART ~]
Context		Contexte	
While hashing and transactions' preimages are required in HTLCs, in Point Time Locked Contracts (PTLCs), transactions are locked using a public key (a *point* on Bitcoin's elliptic curve) and unlocked by providing a corresponding signature from a satisfied signature adaptor. [Teinturier 2024]		Si les HTLC utilisent les empreintes cryptographiques et les pré-images de transactions, dans les contrats à points de verrouillage (PTLC), le verrouillage des transactions nécessite une clé publique (un *point* sur la courbe elliptique de Bitcoin) et le déverrouillage la fourniture d'une signature correspondante obtenue d'un adaptateur de signatures adéquat. [Teinturier 2024, nous traduisons]	

REVOCABLE SEQUENCE MATURITY CONTRACT (RSMC), N. 'cryptographic lock'		**CONTRAT INTELLIGENT RÉVOCABLE À ÉCHÉANCE**, N. masc. 'verrou cryptographique'	
Variant		Variante	
Synonym		Synonyme	
		CONTRAT RSMC	
Definition		Définition	
Smart contract that can be canceled by the sender of funds in case payment conditions are not abided by in an agreed time frame.		Contrat intelligent qui peut être annulé par l'expéditeur de fonds si les conditions de paiement ne sont pas respectées dans le délai convenu.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Cooccurrence		Cooccurrence lexicale	
Realization verb	to bleach [ART ~] to block [ART ~] to renew [ART ~]	Verbe de réalisation	annuler [ART ~] bloquer [ART ~] renouveler [ART ~]
Frequent Expressions		Expressions fréquentes	
security features [of ART ~] HTLC/RSMC-based cross-chain asset swaps		fonctionnalités sécuritaires [de ART ~] échanges interchaînes basés sur les contrats HTLC et RSMC	
Context		Contexte	
The Revocable Sequence Maturity Contract (RSMC), like HTLC, is a smart contract that helps ensure the security and reliability of payments made through the Bitcoin Lightning Network by setting conditions for the release of funds and providing a mechanism for the return of funds if the conditions are not met. [Belchior et al. 2023]		Le contrat intelligent révocable à échéance (RSMC) est, comme le contrat HTLC, un contrat intelligence qui aide à assurer la sécurité et la fiabilité des paiements effectués sur le réseau Bitcoin Lightning en fixant des conditions de paiement de fonds et en mettant en place un Verrou cryptographique pour les retourner à l'expéditeur en cas de non-respect de ces conditions. [Belchior et al. 2023, nous traduisons]	

TO TIMESTAMP, tr. v. 'cryptographic lock'		**HORODATER**, v. tr. 'verrou cryptographique'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
X timestamps Y = X prints on Y the validation date and time of Y.		*X horodate Y* = X imprime sur Y la date et l'heure de validation de Y.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
X = N Y = N, obligatory [The dedicated algorithm (X) timestamps the blocks (Y) while these are validated].		X = N Y = N, obligatoire [La plateforme Solana (X) avait horodaté les transactions (Y) à temps.]	
Lexical Relations		Relations lexicales	
Name for X	timestamp (operator)	Nom pour X	horodateur
Types of Y	block; transaction; transaction data	Types de Y	bloc ; transaction ; données transactionnelles
`Able` adjejctivation	(that can be timestamped)	Adjectivation `Able`	horodatable
Nominalization	timestamping	Nominalisation	horodatage
Context		Contexte	
The blockchain timestamps transaction blocks to enable the development of a timeline map useful for understanding the order during which the transactions occur. [Centobelli *et al.* 2022]		Le réseau horodate les transactions à l'aide d'une fonction de hachage qui les traduit en une chaine d'empreinte continue de preuves de travail. [Rodriguez 2017]	