CLASSE : Preuves cryptographiques [Blockchain]

1. fraud proof (preuve de fraude)
2. PLONK (PLONK)
3. zero-knowledge proof (ZKP) [preuve à divulgation nulle de connaissance ; preuve sans divulgation de connaissance ; preuve zk]
4. ZK-SNARK (zero-knowledge succinct non-interactive of knowledge); ZK-SNARK protocol [ZK-SNARK (preuve succincte non interactive à divulgation nulle) ; argument succinct non interactif à divulgation nulle ; protocole ZK-SNARK ; preuve ZK-SNARK]
5. ZK-STARK (zero-knowledge scalable transparent argument of knowledge) ; ZK-STARK protocol [ZK-STARK (preuve évolutive transparente à divulgation nulle) ; protocole ZK-STARK ; preuve ZK-STARK ; argument succinct non interactif à divulgation nulle]

FRAUD PROOF, N. 'cryptographic proof'		**PREUVE DE FRAUDE**, N. fém. 'preuve cryptographique'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
Cryptographic proof used in optimistic rollups for the execution of a transaction whose validity is challenged by the layer-1 blockchain verifier.		Preuve cryptographique utilisée dans les blockchains de validation groupée optimiste pour l'exécution d'une transaction dont la validité est contestée par le vérificateur de la chaîne principale.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Cooccurrence		Cooccurrence lexicale	
Intensifier	strong	Intensificateur	solide ; robuste ; ⌜en béton⌝
Realization verb	to provi[de ART ~]; to submit [ART ~]	Verbe de réalisation	présenter [ART ~] ; produire [ART ~] ; émettre [ART ~] ; soumettre [ART ~]
Context		Contexte	
In the Ethereum ecosystem, full nodes are allowed to present fraud proofs to light clients – and the entire network at large – as evidence that a transaction is not valid, but this only works well with and may not quite work for danksharding. [Favole 2022]		Côté rollups optimistes, des preuves de fraude sont émises par des agents, généralement des programmes qui observent la blockchain et les transactions des utilisateurs, si le hash placé par un opérateur est frauduleux par rapport aux règles applicatives, et l'opérateur est puni et l'observateur est récompensé. [Augot 2023]	

PLONK, N. 'cryptographic proof'		**PLONK**, N. masc. 'preuve cryptographique'	
Variant		Variante	
Synonym		Synonyme	
Definition		Définition	
ZKP-SNARK-based cryptographic proof that provides a single trusted setup for all circuits and applications and is initiated once and permanently reusable.		Preuve cryptographique basée sur la 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
Confirmer	ZK-SNARK-based	Confirmateur	à ZK-SNARK
Realization verb	to compare [~ *with*] to evaluate [~]	Verbe de réalisation	comparer [~ *avec*] évaluer [~]
Frequent Expressions		Expressions fréquentes	
configuration of confidence [in ~] post-quantic security [of ~] size [of ~] universality [of ~] verification speed [of ~]		niveau de sécurité post-quantique [de ~] taille [de ~] configuration de confiance [de ~] universalité [de ~] rapidité de vérification [de ~]	
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, qui utilise une technique de "dissimulation homomorphique", 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. [Wayne et Piper 2023]	

ZERO-KNOWLEDGE PROOF (ZKP), N. 'cryptographic proof'		**PREUVE À DIVULGATION NULLE DE CONNAISSANCE (ZKP)**, N. fém. 'preuve cryptographique'	
Variant		Variante	
ZK PROOF		PREUVE À DIVULGATION NULLE	
Synonym		Synonyme	
ZERO-KNOWLEDGE PROTOCOL		PREUVE SANS DIVULGATION DE CONNAISSANCE ; PREUVE ZK	
Definition		Définition	
Cryptographic proof that allows a party to prove to another party the completeness, compliance or authenticity of a transaction or related information without revealing any hint.		Preuve cryptographique qui permet à une partie de prouver à une autre partie la complétude, la conformité ou l'authenticité d'une transaction ou d'une information connexe sans rien en dévoiler.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Types of ZKPs	interactive [~] non-interactive [~] three-move honest verifier [~] ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) ZK-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge)	Types de preuves à divulgation nulle	[~] interactive [~] non interactive [~] à trois volets avec vérificateur honnête ZK-SNARK [preuve succincte non interactive à divulgation nulle (= argument succinct non interactif à divulgation nulle)] ZK-STARK (preuve évolutive transparente à divulgation nulle)
Name of result	Transaction data privacy	Nom du résultat	Confidentialité des données transactionnelles
Realization verb	to adopt [ART~] to generate [ART ~] to integrate [ART ~ into/with N] to rely [on ART ~]	Verbe de réalisation	adopter [ART ~] produire [ART ~] ; générer employer [ART ~] intégrer [ART ~ dans N] ; se fier [à ART ~]
Frequent Expressions		Expressions fréquentes	
[~] of knowledge [~] cryptography [~] forgery [~] friendly integer representation [~] system [~] technology ZKP proving time ZKP algorithm increased interest [in ART ~]		argument à divulgation nulle (de connaissance) cryptographie [de ART ~] distorsion [de ART ~] (= manipulation [de ART ~] ; tricherie [dans ART ~]) représentation d'entiers conformément [à ART ~] système [de ART ~] technologie [de ART ~] temps [de ART ~] algorithme [de ART ~] augmentation de l'engouement [pour ART ~]	

privacy-preserving properties [of ART ~]	propriétés [de ART ~] en matière de préservation de la confidentialité
Context	Contexte
For privacy-focused payments and protocols, zero-knowledge proofs (ZKPs) allow a Web3 user, the prover, to prove to the network validators, the verifiers, that their transaction is valid, […] without revealing the transaction details, or the sender or receiver addresses. [Fouda and Wang 2022]	Une preuve à divulgation nulle vous permet de prouver la véracité d'une affirmation sans devoir en partager le contenu ni révéler la manière dont vous avez découvert la vérité ; pour ce faire, le protocole repose sur des algorithmes qui reçoivent certaines données en entrée et renvoient « vrai » ou « faux » en sortie. [Vitalik 2024]

ZK-SNARK (ZERO-KNOWLEDGE SUCCINCT NON-INTERACTIVE ARGUMENT OF KNOWLEDGE), N. 'cryptographic proof'		**ZK-SNARK (PREUVE SUCCINCTE NON INTERACTIVE À DIVULGATION NULLE),** N. fém. 'preuve cryptographique'	
Variant		Variante	
Synonym		Synonyme	
ZK-SNARK PROOF; ZK-SNARK PROTOCOL		PREUVE ZK-SNARK ; PROTOCOLE ZK-SNARK ; ARGUMENT SUCCINCT NON INTERACTIF À DIVULGATION NULLE	
Definition		Définition	
Zero-knowledge proof that is short, robust in terms of privacy and security, and does not require any interaction between the prover and the verifier.		Preuve à divulgation nulle de connaissance qui est brève, robuste en matière de confidentialité et de sécurité, et ne nécessite pas d'interaction entre le prouveur et le vérificateur.	
Syntactic Cooccurrence		Cooccurrence syntaxique	
Lexical Relations		Relations lexicales	
Type of ZK-SNARK	preprocessing [~]	Type de ZK-SNARK	[~] de prétraitement
Realization verb	to apply [ART ~] to generate [ART ~] to verify [ART ~]	Verbe de réalisation	appliquer [ART ~] ; implémenter [ART ~] générer [ART ~] vérifier [ART ~]
Frequent Expressions		Expressions fréquentes	
computational strength [of ART ~] zk-SNARK circuit zk-SNARK functionality zk-SNARK system		puissance de calcul [de ART ~] circuit [de ART ~] fonctionnalité [de ART ~] système [~]	
Context		Contexte	
In the acronym of ZK-SNARK, S implies that the proof size is small which results in processing the transactions quickly and easily, [while] N (Non-interactive) means, no interaction is required with the people who verify the work or transactions. [Moreland 2023]		En plus d'assurer la sécurité et la confidentialité de l'information, la ZK-SNARK (preuve succincte non interactive à divulgation nulle) est plus petite que le témoin [données cachées dont l'existence est censée convaincre davantage le vérificateur] et le prouveur et le vérificateur n'interagissent qu'une seule fois. [Vitalik 2024]	

ZK-STARK (ZERO-KNOWLEDGE SCALABLE TRANSPARENT ARGUMENT OF KNOWLEDGE), N. 'cryptographic proof'	**ZK-STARK (PREUVE ÉVOLUTIVE TRANSPARENTE À DIVULGATION NULLE)**, N. fém. 'preuve cryptographique'
Variant	Variante
Synonym	Synonyme
ZK-STARK PROOF; ZK-STARK PROTOCOL	PREUVE ZK-STARK ; PROTOCOLE ZK-STARK ; ARGUMENT ÉVOLUTIF TRANSPARENT À DIVULGATION NULLE
Definition	Définition
Zero-knowledge proof that more rapidly generates and verifies arguments using a bigger witness and rely on public proving and checking parameters to ensure transparency.	Preuve à divulgation nulle de connaissance qui produit et vérifie plus rapidement les arguments avec un témoin plus volumineux et repose sur des paramètres publics de preuve et de vérification pour garantir la transparence.
Syntactic Cooccurrence	Cooccurrence syntaxique
Lexical Relations	Relations lexicales
Realization verb: to configure [ART ~] to employ [ART ~] to generate [ART ~]	Verbe de réalisation : configurer [ART ~] employer [ART ~] générer [ART ~]
Frequent Expressions	Expressions fréquentes
gas consumption level [of ART ~] proving and checking time [of ART ~] resilience [of ART ~] against quantum computing hacks security and privacy potential [of ART ~]	niveau de consommation de gaz [de ART ~] temps de preuve et de vérification [de ART ~] résistance [de ART ~] contre les attaques quantiques capacités [de ART ~] en matière de sécurité et de confidentialité
Context	Contexte
Transparency and scalability […] account for the most significant differences between zero-knowledge scalable transparent arguments of knowledge (ZK-SNARKs) and zero-knowledge succinct non-interactive arguments of knowledge (ZK-STARKs), in addition to the fact that ZK-STARKs are more secure. [Moreland 2023]	Non seulement la ZK-STARK (preuve évolutive transparente à divulgation nulle) est plus rapide que la ZK-SNARK pour générer et vérifier des preuves avec un témoin de taille plus importante (évolutivité), mais aussi elle repose sur un aléa publiquement vérifiable pour générer les paramètres publics de preuve et de vérification (transparence). [Vitalik 2024]