Anonymat dans les blockchains

Louis de Campou

14/09/2023

Table des matières

1 Introduction

Les échanges financiers sur Internet reposent presque exclusivement via les institutions financières, qui agissent comme tiers de confiance pour le traitement des paiements électroniques.
L'anonymat et la décentralisation sont des caractéristiques intéressantes à explorer pour le futur des paiements électroniques, à cause des inévitables conflits d'intérêt entre les autorités centrales et les utilisateurs.
En 2008, « Bitcoin[1] : A Peer-to-Peer Electronic Cash System » publié sous le pseudonyme Satoshi Nakamoto, a partagé une solution permettant à deux parties d'échanger de la monnaie électronique.
La particularité de cette solution est la suppression de ce modèle de confiance par l'ajout d'une preuve cryptographique.

À ses débuts, Bitcoin a été qualifié comme une monnaie électronique « anonyme » et non pseudonyme. Le pseudonymat de l'utilisateur repose sur l'hypothèse que son pseudonyme, l'adresse d'un compte dérivée à partir d'une paire de clefs, ne soit pas lié à sa véritable identité. D'autres vulnérabilités peuvent être exploitées par un adversaire souhaitant désanonymiser des utilisateurs. Le réseau Bitcoin est un réseau P2P où les participants sont interconnectés via un canal TCP non chiffré. Les participants du réseau, plus connus sous le nom de noeuds, maintiennent à jour une liste d'adresses IP de leurs noeuds voisins. Après qu'une transaction ait été créée, celle-ci est propagée aux noeuds voisins du noeud originaire de la transaction, qui vont eux-mêmes propager la transaction à leurs propres noeuds voisins. Si un noeud contrôlé par un adversaire peut s'assurer qu'une connexion entrante faisant part d'une transaction provient de l'auteur même de la transaction, l'adversaire peut corréler l'adresse IP du noeud et la transaction, compromettant l'anonymat. Une atténuation est d'utiliser un VPN (de confiance !) ou Tor afin d'offusquer sa réelle adresse IP. Un autre risque provient de la nature publique des transactions (voir 2.2) et de l'exploitation du TGA.

Depuis, des protocoles comme CryptoNote[2] à l'origine de Monero, ont émergé mettant l'accent sur la vie privée et l'anonymat. Le TGA n'est plus exploitable car :

- les entrées de transaction ne sont plus liées à un seul émetteur grâce aux signatures en anneau
- une adresse de réception unique est générée par l'émetteur pour chaque transaction grâce aux adresses jetables (« one-time addresses »)
- les montants sont rendus confidentiels grâce à Ring CT

Le prochain chapitre sera consacré à introduire la notion d'espaces de noms (« *namespace* »). L'un des objectifs de ce travail est d'énumérer les espaces de noms en rapport à l'anonymat ainsi que des relations entre espaces de noms pouvant compromettre l'anonymat ou au contraire le garantir.

2 Espaces de noms

Définition 1 (Espace de noms)**.** *Un espace de noms est un ensemble fini d'éléments, qui sont des noms.*

Exemple 1. *Une adresse IPv4 est un espace de noms, composée d'une chaîne binaire de 32 bits, avec un total de* 2^{32} *valeurs.*

Exemple 2. *Une clef publique Bitcoin est un espace de noms, composée d'une chaîne binaire de 256 bits, avec un total de* $2^{256} - 2^{32} - 977$ *valeurs[3].*

Proposition 1 (Composition)**.** *Un espace de noms peut être une composition de deux ou plusieurs espaces de noms.*
Soient 2 espaces de noms A et B, la composition de ces 2 espaces est définie comme un espace de noms C, étant le produit cartésien de A et B : $C = A \times B$

Exemple 3. *Soient A une adresse Bitcoin et B une adresse IP, un portefeuille C hébergé sur une plateforme d'échange peut être représenté tel que :* $C = btc\_addr \times ip\_addr$

Proposition 2 (Résolution)**.** *Un espace de noms peut être résolu en un autre espace de noms. Soient 2 espaces de noms A et B, la résolution de A en B se définit telle que* $\Gamma : A \longrightarrow B$

Exemple 4. *Soient A un nom d'hôte et B une adresse IPv4, le protocole DNS permet de résoudre une adresse IPv4 à partir d'un nom d'hôte ;* $\Gamma : hostname \longrightarrow ip\_addr$

2.1 Adresse Bitcoin & Monero

Dans le contexte d'une *blockchain*, une adresse est un espace de noms qui sert de mécanisme de routage dans un système distribué. Une adresse Bitcoin[4] (P2PKH) est composée de 160 bits. Un espace d'adressage fait référence au nombre d'adresses disponibles dans un espace donné, il est de 2^{160} pour une adresse Bitcoin. Chaque adresse, étant la sortie du haché de la clef publique correspondante, peut être considérée comme une clé unique.

Les adresses Bitcoin & Monero[5, 6] sont définies ci-dessous respectivement.
G représente un point de base de la courbe elliptique (secp256k1[3] pour Bitcoin et Ed25519[2, p. 5] pour Monero).

espace	taille en bits	description
priv key k	256	génération de bits pseudo-aléatoire
pub key K	256	$K = kG$
address	160	base58(0x00 + ripemd160(sha256(K)) + checksum)
balance		UTXO

Table 1 – Adresse Bitcoin

espace	taille en bits	description
priv spend key k^s	256	génération de bits pseudo-aléatoire
priv view key k^v	256	$k^v = H(k^s)$
pub spend key K^s	256	$K^s = k^s G$
pub view key K^v	256	$K^v = k^v G$
address	552	base58(0x12 + $K^s \| \| K^v$ + checksum)
open alias		nom d'hôte associé à une adresse
balance		UTXO

Table 2 – Adresse Monero

La somme de contrôle d'une adresse Bitcoin est égale à : sha256(sha256(0x00 + ripemd160(sha256(K))))[0 :31]
La somme de contrôle d'une adresse Monero est égale à : keccak256(0x18 + K)[0 :31]

- Les clefs Monero sont deux fois plus grandes que les clefs Bitcoin
- Les adresses Monero possèdent 392 bits de plus que les adresses Bitcoin
- Monero scinde les clefs en 2 usages : « *spend* » pour défenser des fonds et « *view* » pour obtenir le solde et l'historique de transactions d'une adresse
- Le solde et l'historique de transactions d'une adresse Bitcoin sont publiques. Contrairement à Monero, où l'on peut choisir de communiquer k_v
- Dans une transaction Bitcoin, les adresses et les montants associés sont publiques tandis que Monero anonymise ces informations.

2.2 Transaction Bitcoin & Monero

Une transaction (« tx ») est un objet contenant plusieurs champs dont certains champs sont des espaces de noms (adresse) et d'autres sont des métadonnées (horodatage).

Une transaction représente un mouvement de monnaie d'une adresse à une autre, signée avec la clef privée de l'expéditeur, qui souhaite réattribuer la possession d'une certaine quantité de monnaie à une adresse de destination spécifiée dans la transaction.
Plus précisément, une transaction consiste en :

— un ensemble d'entrées (UTXO). Chaque entrée contient un montant associé
— un ensemble de sorties ou d'adresses de destination
— un montant à transférer à chaque sortie

Les transactions Bitcoin & Monero sont définis ci-dessous respectivement.

espace	taille en bits	description
hash	256	haché de la transaction
input	160	adresse(s) d'entrée
output	160	adresse(s) de sortie
value		montants associés aux adresses d'entrée et de sortie
signature		preuve que l'expéditeur a autorisé la transaction

Table 3 – Transaction Bitcoin

espace	taille en bits	description
hash	256	haché de la transaction
input	256	image(s) clé(s)
output	256	adresse(s) jetable(s)
payment id	64	chaîne de caractères unique permettant d'identifier une transaction
ring signature		preuve que l'expéditeur a autorisé la transaction

Table 4 – Transaction Monero

3 Méthodes d'anonymat

Soit un ensemble d'agents $(A_1, ..., A_n)$ qui s'échangent des messages sur un canal de communication par défaut unidirectionnel (et bidirectionnel lorsque précisé). Un agent peut être un émetteur ou/et un récepteur. Tout message transite vers un système d'anonymat dans un modèle de boîte noire. Selon la nature de la méthode d'anonymat utilisée, un agent peut être dénoté par une adresse IP, une clef publique.. Le canal de communication est surveillé par un observateur, qui souhaite par exemple connaître l'identité de l'émetteur ou du récepteur d'un message. Cet observateur est un adversaire honnête mais curieux[7, p. 2], un participant légitime qui ne s'écarte pas du protocole défini mais tente d'obtenir toutes les informations possibles à partir des messages reçus légitimement. Les *blockchains* Bitcoin et Monero étant publiques, l'observateur a accès possiblement en lecture à toutes les transactions publiées sur ces registres. On s'intéressera principalement à l'anonymat de l'émetteur, le principe est analogue pour l'anonymat du récepteur. L'anonymat de l'émetteur consiste à être indistinguable[8] au sein d'un ensemble, l'ensemble d'anonymat (« *anonymity set* »). Il y a un ensemble d'émetteurs possibles et l'observateur ne peut pas faire la distinction entre les émetteurs de cet ensemble. L'observateur souhaite connaître quel émetteur parmi l'ensemble d'anonymat est à l'origine d'un message, il assigne une probabilité pour chaque émetteur. Deux méthodes d'anonymat sont analysées : les adresses jetables et les signatures en anneau.
D'autres méthodes auraient pu être explorées :

— Mixeur : service qui permet d'offusquer la relation entre entrées et sorties d'une transaction, et préserver l'anonymat relationnel. Ce service peut être centralisé, c'est à dire qu'il dépend d'un serveur central pour effectuer le mixing. Un problème de confiance est inhérent avec cette approche : il n'y

a aucune certitude que ce type de service ne conserve des logs (adresses *blockchain*, adresses IP..) ou redistribue les jetons.
— Tor (le routage en oignon) : réseau superposé et distribué permettant d'anonymiser les applications basées sur le protocole TCP. Chaque utilisateur (« *onion proxy* ») choisit un chemin à travers le réseau et construit un circuit, dans lequel chaque noeud (« *onion router* ») connaît uniquement son prédecesseur et son successeur dans celui-ci.
— VPN IPsec mode tunnel

3.1 Adresse jetable

Les adresses jetables sont des adresses pseudo-aléatoires à usage unique, générées par l'expéditeur pour chaque transaction, permettant de masquer l'adresse du destinataire. Le destinataire publie une seule adresse mais tous ses paiements entrants sont adressés à des adresses uniques, elles ne peuvent pas être liées à l'adresse du destinataire. La propriété de non-liaison[2, p. 1] (« *unlinkability* ») est satisfaite : pour deux transactions sortantes, il est impossible de prouver qu'elles ont été envoyées à la même adresse.

H_s : une fonction de hachage cryptographique $\{0,1\}^* \to \mathbb{F}_q$
G : Point de base de la courbe Ed25519
$l = 2^{252} + 27742317777372353535851937790883648493$

1. Alice génère $r \in [1, l-1]$
2. Alice calcule l'adresse jetable correspondante : $S = H_s(rK_b^v)G + K_b^s$
3. Alice envoie une transaction avec S comme destinataire (contenant R=rG)
4. Bob vérifie toutes les transactions qui transitent sur le réseau et calcule : $S' = H_s(Rk_b^v)G + K_b^s$
5. Bob consomme la sortie si $S = S'$ ($R\,k_b^v = rG\,k_b^v = rK_b^v$)
6. Bob peut dépenser cette sortie en signant la transaction avec $x = H_s(Rk_b^v) + k_b^s$

Lorsque Bob vérifie qu'une transaction lui appartient, il effectue 2 multiplations et une addition sur la courbe elliptique par sortie. Du point de vue de l'observateur, il n'a connaissance ni de r, ni de k_b^v et il n'est pas en capacité de résoudre le problème du logarithme discret appliqué aux courbes elliptiques (ECDLP). Sous ces hypothèses, l'observateur est en incapacité de connaître le récepteur du message et de résoudre l'adresse de Bob à partir de l'adresse jetable générée par Alice.

Proposition 3. *Soient 2 agents A_1 et A_2, A_1 envoie un message à A_2 via une adresse jetable : $A_1 \to S$*
Une adresse jetable garantit un anonymat α_1 du récepteur si la résolution suivante est difficile : $\Gamma := S \mapsto A_2$

3.2 Signature en anneau

Une signature en anneau est composée d'un anneau et d'une signature. Un anneau est un ensemble de clefs publiques dont l'une appartient au signataire. La signature est générée à l'aide de cet anneau, et toute personne qui la vérifierait ne pourrait pas savoir quel membre de l'anneau est le véritable signataire.
Une signature en anneau d'un message m avec les clefs publiques $\{K_1, K_2, ..., K_n\}$ prouve qu'une personne ayant connaissance de l'une des clefs privées $\{k_1, k_2, ..., k_n\}$ a signé le message m.
Une signature en anneau est utilisée pour anonymiser l'identité de l'expéditeur parmi un nombre de signataires potentiels. Les entrées de la transaction (UTXO) sont cachées dans un anneau. Une image clef (*« key image »*) associée à une signature en anneau garantit que, même si on ne peut pas déterminer la source d'une transaction, il est façile de vérifier si l'expéditeur a tenté d'envoyer les mêmes fonds plusieurs fois (problème de la double dépense). La propriété d'intraçabilité[2, p. 1] (« *untraceability* ») est satisfaite : pour chaque transaction entrante, tous les expéditeurs possibles sont équiprobables.
Plus la taille de l'anneau est grand, plus la propriété d'intraçabilité est forte.
Du point de vue de l'observateur, il peut résoudre un ensemble de clefs publiques à partir de la signature

$(\Gamma := \sigma \mapsto \{K_1, K_2, ..., K_n\})$.
Son objectif est de déterminer l'index π du réel signataire parmi $\{K_1, K_2, ..., K_n\}$.

H_p : une fonction de hachage déterministe $\mathrm{E}(\mathbb{F}_q) \to E(\mathbb{F}_q)$

Une signature en anneau contient 4 algorithmes :

- GEN : le signataire génère $x \in [l-1]$, calcule la clef publique $P = xG$ et l'image clef correspondante $I = xH_p(P)$ [1]
- SIG : prend un message m, un ensemble S' de clefs publiques $P_i (i \neq \pi)$, une paire (P_π, x_π) et produit une signature σ et un ensemble $S = S' \cup P_\pi$
- VER : prend un message m, un ensemble S, une signature σ et indique en sortie "vrai" ou "faux"
- LNK : prend un ensemble $\mathcal{I} = \{I_i\}$ et vérifie si I est contenue dans l'ensemble : lorsqu'une nouvelle transaction est émise sur le réseau, sa signature est vérifiée (VER). Si la signature est correcte, l'image clef de la transaction est comparée aux éléments de l'ensemble, noté $\mathcal{I}$, des images clefs de toutes les transactions passées. Si l'image clef appartient à $\mathcal{I}$, cela signifie que le signataire a effectué une double dépense et la transaction est refusée. Sinon, l'image clef est ajoutée à $\mathcal{I}$ et la transaction est acceptée.

Proposition 4. *Une signature en anneau garantit un anonymat α_2 de l'émetteur si la résolution suivante est difficile :* $\Gamma := A \mapsto A_1$.

4 Mesure de l'anonymat

Un système de communication anonyme idéal a un ensemble d'anonymat égal au nombre d'agents du système et la probabilité de chaque agent étant à l'origine du message est égal, c'est à dire que la distribution est uniforme. Pour quantifier l'anonymat, il faut donc prendre en compte la cardinalité (le nombre d'agents dans le système) et la distribution des probabilités. L'entropie est un terme emprunté à la thernodynamique qui est une mesure du désordre ou d'incertitude d'un système. Après la seconde guerre mondiale, Claude Shannon a théorisé mathématiquement l'entropie. Si la probabilité que l'agent i soit l'émetteur du message est p_i, et qu'il y a N agents dans l'ensemble d'anonymat, alors l'entropie de l'ensemble d'anonymat S est :

Définition 2 (Entropie de Shannon[9]). $H(S) = -\sum_{i=1}^{N} p_i log_2(p_i)$

L'entropie de Shannon décrit l'imprévisibilité moyenne des résultats d'un système, elle est bornée par : $0 \leq H(S) \leq log_2(N)$

L'entropie normalisée est dérivée de l'entropie de Shannon, elle examine le ratio entre le sécurité d'un système idéal pour une base d'utilisateurs et la sécurité réelle du système pour la même base d'utilisateurs. Elle est donc bornée par : $0 \leq d \leq 1$

Définition 3 (Entropie normalisée[10]). $d = \frac{H(S)}{log_2(N)}$

Si l'on prend l'exemple d'une signature en anneau Monero de taille 16, par la propriété d'intraçabilité, les 16 émetteurs sont équiprobables du point de vue d'un observateur.

$H(S) = log_2(16) = 4$
$d = 1$

Cependant, il peut exister des distributions de même cardinalité dont les distributions de probabilités sont différentes mais qui résultent par la même entropie de Shannon et donc la même entropie normalisée. On peut se poser la question parmi ces distributions, quelle est la plus vulnérable dans le cas d'un observateur capable d'enquêter uniquement sur un seul émetteur.

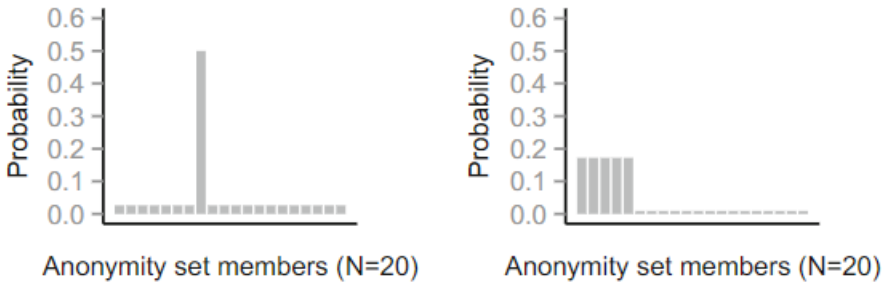

FIGURE 1 – Deux distributions[10][9] avec la même cardinalité (≈ 4.32 bits), la même entropie de Shannon (≈ 3.12 bits) et la même entropie normalisée (≈ 0.72)

La distribution de gauche a un émetteur avec une probabilité de $\frac{1}{2}$ et les 19 autres avec une probabilité de $\frac{1}{38}$. La distribution de droite a 5 émetteurs avec une probabilité de $\frac{a}{5}$ et les 15 autres avec une probabilité de $\frac{1-a}{15}$ où $a \approx 0.86$ est la solution de l'équation définie par Toth dans « Measuring anonymity revisited ». Un observateur capable d'enquêter uniquement un seul émetteur a une chance de réussite de 50% dans la distribution de gauche et de 17.2% dans celle de droite. D'où l'utilisation de la min-entropie, une mesure conservatrice qui décrit l'imprévisibilité d'un résultat déterminé par la probabilité du résultat le plus probable. Cela correspond à la sécurité effective dans le cas d'un observateur capable d'enquêter sur un seul émetteur. La min-entropie de la distribution de gauche est de 1 bit et celle de droite de ≈ 2.54 bits. Du point de vue du concepteur d'un système, on privilègera donc la distribution de droite à celle de gauche.

Définition 4 (Min-entropie)**.** $H_{min}(S) = -log_2(max\, p_i)$

5 Tableau de niveau de protection

	Bitcoin	Monero	Comment ? (Monero)
Anonymat de l'émetteur	Non	Oui (1/16)	Signature en anneau
Anonymat du récepteur	Non	Oui	Adresse jetable
Confidentialité des montants	Non	Oui	Ring CT
Révélation adresse IP	?	Non	Dandelion ++
Résistance au TGA	Non	Oui	Signature en anneau, adresse jetable, Ring CT

Glossaire

blockchain une base de données distribuée constituée d'une chaîne de blocs liés et sécurisés par des hachés cryptographiques.. 4, 5

DNS Domain name system. 4

ECDLP Elliptic curves discrete logarithm problem. 6

IP Internet Protocol. 3–6, 8

P2P Pair à pair. 3

P2PKH Pay-to-Public-Key-Hash. 4

Ring CT Ring Confidential Transactions. 3, 8

TCP Transmission Control Protocol. 3, 6

TGA Transaction graph analysis. 3, 8

Tor The Onion Router. 3, 6

UTXO Somme des sorties non dépensées (« *unspent transactions outputs* »). 4–6

VPN Virtual Private Network. 3, 6

Références

[1] Satoshi Nakamoto. *Bitcoin : A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf.

[2] Nicolas van Saberhagen. *CryptoNote v2.0.* https://bytecoin.org/old/whitepaper.pdf.

[3] Bitcoin Wiki. *Secp256k1.* https://en.bitcoin.it/wiki/Secp256k1.

[4] Bitcoin Wiki. *Technical background of version 1 Bitcoin addresses.* https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses.

[5] *Monero address cheatsheet.* https://www.getmonero.org/library/MoneroAddressesCheatsheet20201206.pdf.

[6] *Monero documentation : Standard address.* https://monerodocs.org/public-address/standard-address/.

[7] Ian Brown Andrew Paverd Andrew Martin. *Modelling and Automatically Analysing Privacy Properties for Honest-but-Curious Adversaries.* https://www.cs.ox.ac.uk/people/andrew.paverd/casper/casper-privacy-report.pdf.

[8] Marit Hansen Andreas Pfitzmann. *A terminology for talking about privacy by data minimization : Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management.* https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

[9] Claudia Diaz et al. "Towards measuring anonymity". In : *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002).* Sous la dir. de Roger Dingledine et Paul Syverson. Springer-Verlag, LNCS 2482, avr. 2002.

[10] Steven J. Murdoch. *Quantifying and Measuring Anonymity.* https://murdoch.is/papers/dpm13quantify.pdf.