

UNIVERSITÉ DE LAUSANNE

MÉMOIRE DE MASTER

**Identités en confrontation : confiance et
anonymat au sein des *darknet markets***

Auteur :
Arnaud STEPHAN

Superviseur :
Boris BEAUDE
Expert :
Olivier GLASSEY

*Mémoire soumis dans le cadre
du diplôme de Master en
Humanités Numériques*

Session d'Automne 2018

The logo of the University of Lausanne (UNIL) is a stylized, cursive script in blue, consisting of the letters 'Unil'.

UNIL | Université de Lausanne

Faculté des lettres

« L'expérience prouve que celui qui n'a jamais confiance en personne ne sera jamais déçu. »

Léonard de Vinci

UNIVERSITÉ DE LAUSANNE

Abstract

Master en Humanités Numériques

Identités en confrontation : confiance et anonymat au sein des *darknet markets*

par Arnaud STEPHAN

Ce travail porte sur les *darknet markets*, places de marché en ligne sur lesquelles il est possible de se procurer, entre autre, de nombreux produits illicites. Lieux où l'anonymat est de mise, ces plateformes n'ont à priori d'autre choix que de faire apparaître des relations de confiance entre leurs utilisateurs pour fonctionner. Il s'agit là d'une situation paradoxale, étant donné l'incompatibilité que l'on peut imaginer entre confiance et anonymat. En étudiant la manière dont les technologies et les pratiques sociales facilitent l'apparition et la conservation de la confiance, ainsi que la façon dont les forces de l'ordre s'attaquent à ces marchés, nous tentons de déterminer s'il est effectivement possible d'instaurer des relations de confiance sur de telles plateformes.

Remerciements

Mes premiers remerciements vont à Olivier Glassey, pour m'avoir aiguillé lors de mes recherches préliminaires en me conseillant des ouvrages qui se sont révélés déterminants lors de ce travail. Merci également à Boris Beaude pour m'avoir épaulé au cours de ma rédaction, et pour avoir pris le temps de répondre à mes questions.

Merci mille fois à Jeanne, Célia, Jeremie, Manon et Ariane pour leur soutien tout au long de ce travail et plus généralement leur compagnie dès la première année de bachelor.

Merci ensuite aux gens du camping de Poulfoen pour m'avoir soutenu au cours de ma dernière semaine de rédaction. La salle multimédia/vaisselle/lessive fut témoin de leurs efforts conjugués.

Merci enfin à ma famille et plus particulièrement à mes parents, qui m'ont soutenu tout au long de mon long et enrichissant parcours d'éternel étudiant. Ce fut leur soutien inébranlable lors de mon changement de parcours qui me permet aujourd'hui d'être diplômé.

Table des matières

Abstract	iii
Remerciements	iv
1 Introduction	1
1.1 La confiance comme point de passage obligé	2
1.2 Définitions	4
1.2.1 Darknet, deep web ou dark web?	4
1.2.2 Identité & anonymat	5
2 La notion de confiance	7
2.1 Son rôle dans les interactions	8
2.1.1 Mécanisme de réduction de la complexité sociale	8
2.1.2 Le problème de la double contingence	9
2.2 Confiance et nouvelles technologies	10
2.2.1 Modalisation de la confiance à travers les NTIC	10
2.2.2 La <i>digital trust</i> : une utopie?	12
3 Darknet & <i>marketplaces</i>	15
3.1 Historique	15
3.1.1 Silk Road	16
3.1.2 L'âge d'or des DNMs	19
3.2 <i>Operation Bayonet</i> et ses conséquences	21
3.2.1 La destruction du PPO	21
3.2.2 Reconfiguration du schéma de problématisation	24
3.2.3 État des lieux	25
4 La création du lien de confiance sur les DNMs	28
4.1 Via les pratiques	28
4.1.1 Identité digitale	28
4.1.2 Évaluations & réputation	31
4.1.3 Documents d'identité et tiers de confiance	35
4.2 Via les technologies	37
4.2.1 Moyens d'accéder au réseau (TOR)	37
4.2.2 Systèmes d'exploitation	39
4.2.3 Communications chiffrées et identités persistantes	40

4.2.4	Cryptomonnaies	41
4.3	Limites	43
4.3.1	Sociales	43
4.3.2	Inhérentes aux technologies utilisées	44
5	Conclusion	46
5.1	Familiarité ou confiance?	46
5.2	De l'importance des maillons faibles	47
5.3	Point de Passage Obligé?	48
A	Entretiens	50
A.1	_da_da_da	50
A.2	pouetpouet123456	52
A.3	organichewn	53
	Références	56

Table des figures

1.1	Problématisation du fonctionnement des DNMs	3
2.1	Les évaluations sur DHL	13
3.1	Cours du BTC début 2011	17
3.2	Silk Road post Marco Polo	17
3.3	frosty, lien entre Ross Ulbricht et Silk Road	18
3.4	Le faisceau des liens reliant Ross Ulbricht à Silk Road	19
3.5	La page d'accueil d'AlphaBay après Operation Bayonet	22
3.6	Les DNMs sans PPO	23
3.7	Message de DHL	24
3.8	Prise de conscience de la véritable configuration	24
3.9	Evolution du nombre de listings sur Aero	26
4.1	Transfert d'identité de pseudo à pseudo	29
4.2	Un revendeur de pilules de MDMA produites par CP	30
4.3	La réputation sur Dream Market	32
4.4	La réputation sur Dream Market - 2	33
4.5	La réputation sur Dream Market - 3	33
4.6	Interface de <i>dispute</i> sur AlphaBay	34
4.7	Nice try officer	35
4.8	Energy Control comme gage de qualité	37
4.9	L'interface de connexion à Tor	38
4.10	Evolution de la bande passante de Tor	38
4.11	Une clef PGP publique	40
4.12	Un extrait de la blockchain du Bitcoin	42

Liste des abréviations

BTC	Bitcoin
DD	Direct Deal
DNM	DarkNet Market
DPR	Dread Pirate Roberts
FE	Finalize Early
LE	Law Enforcement
LEO	Law Enforcement Officer
PGP	Pretty Good Privacy
SR	Silk Road
TAILS	The Amnesic Incognito Live System
TFM	The Farmer's Market
TOR	The Onion Router
XMR	Monero

1 Introduction

« There is no place for anonymity in a trusted community. [...] Trust and verification. They just go together. »

En 2013, AirBnB introduisait par ces mots son système de *Verified ID*,¹ permettant de régler l'un des principaux problèmes de la plateforme : la confiance. Sur ces sites pratiquant le « prêt payant » (JACQUET, 2015), la question de la bienveillance des utilisateurs est en effet un obstacle majeur à l'adoption de ces nouvelles pratiques. La question qui se pose est souvent la suivante : Comment puis-je m'assurer que l'inconnu à qui je loue mon appartement, ou avec lequel je monte en voiture, va bien remplir sa part du contrat ?

La plupart des plateformes servant de cadre à des échanges de services ou de bien commerciaux entre particuliers ont aujourd'hui recours à des versions plus ou moins poussées d'un système de vérification d'identité : AirBnB a son système de *Verified ID*, Alibaba propose le badge *Assessed Supplier*,² et les utilisateurs de BlaBlaCar peuvent atteindre cinq niveaux d'expérience,³ le passage de l'un à l'autre se faisant en remplissant des conditions de plus en plus exigeantes. La constante de tous ces systèmes est la volonté pour les plateformes les ayant mis en place de faire le lien entre l'identité numérique et l'identité civile de leurs utilisateurs, afin de diminuer le nombre de "brebis galeuses".

Au cours de ce mémoire, nous nous intéresserons au darknet,⁴ et plus particulièrement aux places de marché sur lesquelles il est possible de se procurer des substances illicites. On comprend aisément que, contrairement aux plateformes classiques mentionnées plus haut, le lien entre identité civile et numérique est proscrit sur ces places de marché. De nombreuses stratégies - technologiques ou sociales - sont alors mises en place par les utilisateurs afin d'échapper aux forces de l'ordre et de créer un entre-soi protégé où il est possible de discuter de ces stratégies.

1. <https://goo.gl/oAZF4g>, accédé le 06.07.2018

2. <https://goo.gl/S9Uaab>, accédé le 06.07.2018

3. <https://goo.gl/am4Gis>, accédé le 06.07.2018

4. Cette notion sera définie plus bas

1.1 La confiance comme point de passage obligé

Lorsque l'on s'intéresse aux marchés du darknet, un paradoxe saute aux yeux : il est primordial pour chaque utilisateur de camoufler sa véritable identité, mais il est tout autant indispensable de pouvoir faire confiance aux différents acteurs tout au long du processus d'achat.

S'il est déjà compliqué de créer des relations de confiance dans des interactions en face à face, cette complexité augmente encore avec l'ajout de la dimension numérique. On ne doit alors plus simplement faire confiance à la personne avec laquelle on interagit, mais également confiance à la technologie utilisée pour communiquer : « Establishing a trust relationship in digital networking environments involves more aspects than in the social world. This is because communications in the computing network rely on not only relevant human beings and their relationships, but also digital components » (YAN et HOLTMANNS, 2008, p. 3).

De plus, ces relations de confiance qui se créent sur le darknet ne sont pas *one to one*, pour reprendre un terme employé en informatique, mais *one to many*. Chaque acteur interagit en effet avec plusieurs autres acteurs au cours de l'utilisation de ces réseaux : un acheteur "lambda" doit tout d'abord sélectionner un marché parmi d'autres, puis un vendeur spécifique au sein de tous les vendeurs présents sur ce marché. Et, pour s'aider dans son choix, il peut lire les évaluations laissées aux vendeurs par d'autres acheteurs comme lui.

L'utilisation de ces plateformes, si elle se passe sans heurts dans la plupart des cas, peut toutefois avoir des conséquences dramatiques pour leurs utilisateurs. Judiciaires en premier lieu, s'ils ont laissé suffisamment de traces pour permettre aux forces de l'ordre d'accumuler assez de preuves quant à leurs achats de substances illicites ; ou de graves problèmes de santé, si la substance achetée à un vendeur était contaminée, trop dosée, voire tout simplement différente de ce qui était affiché au moment de la commande. Compte tenu des conséquences potentiellement néfastes, et le faible bénéfice qui se retrouve alors associé à un risque énorme, nous pouvons nous poser une première série de questions afin d'orienter notre réflexion :

Comment cela se fait-il que les marchés du darknet fonctionnent aussi bien ? De quelle façon est-ce que des acteurs qui ne se connaissent pas et ne se rencontreront jamais arrivent-ils à créer des réseaux mondiaux de coopération aussi efficaces, en étant conscients des risques que cela implique ? Est-il réellement possible de créer des relations de confiance sur des plateformes où l'anonymat est aussi prépondérant ?

En nous inspirant de la recherche de Michel Callon sur les pêcheurs dans la baie de Saint-Brieuc (1986), nous pouvons schématiser cette problématique via le schéma de la figure 1.1.

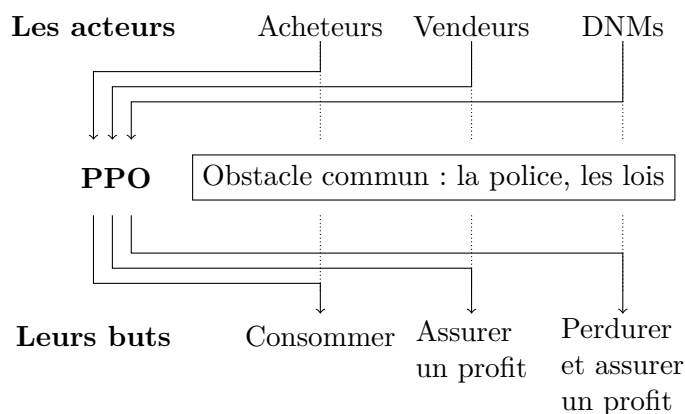


FIGURE 1.1 – Problématisation du fonctionnement des DNMs

Si l'on considère les trois types principaux d'acteurs impliqués dans l'utilisation de ces plateformes -acheteurs, vendeurs, et DNMs-, ce schéma nous permet de mieux visualiser les dynamiques sociales à l'œuvre. Ce que visent ces acteurs, « ils ne peuvent l'atteindre par eux-mêmes » (ibid., p. 183), et cela les oblige à passer par un point de passage obligé (PPO) : faire confiance. Se faire confiance mutuellement, mais également à d'autres entités non représentées sur le schéma : développeurs des logiciels utilisés, fabricants de matériel, fournisseurs d'accès à Internet, etc. C'est ce PPO qui va permettre à tout un chacun d'éviter d'être pris dans les mailles du filet de la justice, ou en tout cas d'en minimiser la probabilité.

Pour répondre à la problématique exposée plus haut, nous étudierons en premier lieu la notion même de confiance. Quelle est son utilité sociale, comment apparaît ou disparaît elle, et quels sont les moyens d'assurer sa longévité ? Nous mobiliserons principalement dans cette partie les ouvrages de Rachel Botsman (2017) et Niklas Luhmann (2006b), ainsi que le recueil de Albert Ogien & Louis Quéré (2006). Nous verrons également en quoi la technologie peut jouer un rôle dans ce processus, notamment avec l'émergence récente de la notion de *digital trust*.

Dans une seconde partie, nous nous intéresserons au fonctionnement de l'écosystème des DNMs au sein du darknet. Après un rappel historique nous nous pencherons plus particulièrement sur la récente *Operation Bayonet* et ses conséquences, et nous procéderons à une étude de cas sur deux DNMs en particulier : TradeRoute et Aero. aujourd'hui défunts. Nous finirons par un état des lieux, qui sera également l'occasion de nous rendre compte que ce PPO est un point stratégique non seulement pour les utilisateurs des DNMs mais également pour les forces de l'ordre.

Enfin, nous mettrons en lien ces deux premières parties pour comprendre comment le darknet peut être, ou non, un générateur de confiance : nous passerons en revue pour cela les technologies utilisées ainsi que les pratiques mises en œuvre pour atteindre le PPO, élément central de ce travail.

Pour conclure, nous montrerons que ce que l'on prend pour de la confiance pourrait en

réalité être de la familiarité, et ce d'autant plus sur le darknet. Nous verrons également que la confiance peut être un point de passage optimal plutôt qu'obligé, et en quoi cela modifie les pratiques des utilisateurs.

Avant de passer à la suite de ce travail, une précision semble importante. La recherche sur un milieu aussi mouvant qu'Internet s'avère souvent compliquée, surtout lorsque le terrain étudié se situe aux frontières de la légalité. La plupart des DNMs qui seront mentionnés plus bas n'existent aujourd'hui plus, de même que certaines plateformes. C'est notamment le cas du subreddit /r/DarknetMarkets, sur lequel de nombreuses observations ont été réalisées à partir de début 2017. Ce subreddit, comme beaucoup d'autres liés aux DNMs, a été banni par les administrateurs du site le 21 mars 2018 dans le cadre d'une modification des conditions générales d'utilisation de la plateforme.⁵

Ainsi, les traces sur lesquelles se basent ce travail existent sous deux formes : des captures d'écran d'interactions intéressantes effectuées au fil des mois, ainsi qu'une archive HTML de /r/DarnetMarkets réalisée par l'utilisateur gwern⁶ et mise à disposition du public après le 21 mars 2018.⁷ Un des points centraux de la méthode scientifique étant la reproductibilité des observations et des résultats, ceci est ici impossible. Rien ne prouve que gwern n'a pas modifié l'archive avant de la mettre à disposition, de même que rien ne prouve que le code source des pages n'a pas été modifié avant d'en prendre des captures d'écran.

Toutefois, si certaines des interactions qui seront présentées aujourd'hui ne sont plus disponibles en ligne et dans leur contexte d'origine, les analyses qui en découlent n'en sont pas pour autant invalidées. Les DNMs existent encore aujourd'hui, tout autant que les plateformes d'échanges entre utilisateurs. Ces plateformes sont accessibles publiquement, et chacun peut se rendre compte par lui-même que ce qui est décrit dans ce travail est encore valable aujourd'hui.

1.2 Définitions

1.2.1 Darknet, deep web ou dark web ?

Avant de nous intéresser à la question du darknet, il est primordial de définir ce que nous entendons par ce concept. Il peut en effet prêter à confusion, d'autant plus que différentes significations s'y retrouvent imbriqués : on peut ainsi entendre parler de dark net, mais également de dark web, hidden web, ou encore deep web. De nombreuses tentatives de définitions existent, et nous nous baserons ici sur celles du Journal officiel du 26 septembre 2017.⁸

5. L'annonce est accessible ici : <https://goo.gl/4QJXgG>, accédé le 20.07.2018

6. <https://goo.gl/WZhxaM>

7. Téléchargeable ici : <https://goo.gl/EJ8bn5>, accédé le 20.07.2018

8. <https://goo.gl/2JKrW1>, accédé le 06.07.2018

Darknet Ensemble de réseaux conçus pour assurer l’anonymat des utilisateurs par la mise en œuvre d’une architecture décentralisée ainsi que de logiciels et d’autorisations d’accès spécifiques ; par extension, l’ensemble des activités, souvent illicites, qui y sont pratiquées.

Deep web Partie de la toile qui n’est pas accessible aux internautes au moyen des moteurs de recherche usuels.

Cette définition est toutefois problématique : le darknet serait le théâtre d’activités « souvent illicites », mais de nombreux sites ayant des activités illégales sont hébergés sur le web classique : c’est par exemple le cas de la plupart des sites vendant des contrefaçons. Inversement, certaines ONG tout à fait légitimes sont hébergées sur le darknet afin d’assurer la sécurité de leurs utilisateurs ou contributeurs.⁹

Le deep web quant à lui, qui n’est pas indexé par les moteurs de recherche usuels, devient une notion bien trop générale : n’importe quelle page non accessible aux robots de ces moteurs fait ici partie du deep web, qu’il s’agisse d’un groupe Facebook privé ou d’une boîte mail.

Ces deux définitions permettent néanmoins, dans le cadre de ce travail, de savoir de quoi l’on parle : un *darknet market* est une place de marché du deep web, à laquelle on accède en passant par le darknet. Certaines places de marché sont présentes sur le web classique : nous choisissons de ne pas les prendre en compte dans ce travail. Leur utilisation n’est en effet pas recommandée par la communauté des utilisateurs car ne pas passer par le darknet est une immense faille en matière de sécurité opérationnelle, comme nous le verrons lors du chapitre 4.

1.2.2 Identité & anonymat

Concernant ces deux notions, là encore un travail d’explicitation s’impose. Si on entend habituellement par identité l’identité sociale d’un individu, c’est à dire celle délivrée par un État, cette définition ne suffit plus dans le cadre de ce travail. Il est en effet possible aujourd’hui de changer d’identité numérique très facilement, qu’il s’agisse d’une identité potentiellement persistante (pseudonyme dans une salle de discussion, compte sur un réseau social), ou destinée à n’être que temporaire (adresse IP, adresse MAC, taille de la fenêtre du navigateur, etc.).

Les définitions proposées par Camp et Lecomte nous sont ici très utiles :

Attribut Caractéristique associée à une entité, par exemple un individu. On peut citer la couleur des yeux ou la date de naissance comme attributs permanents,

9. Le cas de WikiLeaks est le plus connu : <https://goo.gl/WRfLWi>, accédé le 06.07.2018

l'adresse ou la fonction comme attributs temporaires, et le numéro de sécurité sociale comme attribut long terme.¹⁰ (CAMP, 2004, p. 35)

Identité L'ensemble des attributs qui sont associés de manière permanente ou sur le long terme à une entité.¹¹ (ibid., p. 36)

Identifiant Un identifiant permet de singulariser une personne, un endroit ou une chose dans le cadre d'un espace de noms. [...] Une personne, un endroit ou une chose peuvent avoir plusieurs identifiants. [...] Chaque identifiant n'a de sens que dans cet espace de noms, et seulement lorsqu'il est associé avec l'entité qu'il identifie.¹² (ibid., p. 35)

Anonyme Un individu est anonyme lorsque les attributs qui lui sont associés ne correspondent pas à un identifiant. Lorsque les attributs sont associés plusieurs fois à une même identité anonyme, on parle de pseudonyme.¹³ (ibid., p. 36)

Identité numérique Ensemble des informations, des données personnelles [...], et surtout des contributions et autres actions publiques [...] laissées sur Internet par un même utilisateur [...] constituant autant de "traces" accumulées dessinant les contours d'une identité en ligne. (LECOMTE, 2010, p. 64)

Dans le cadre étudié ici, les DNMs, il va de soi que les utilisateurs n'ont aucun intérêt à utiliser des attributs pouvant permettre de remonter jusqu'à eux. Le but est d'être le plus anonyme possible, et ce travail d'anonymisation porte alors sur plusieurs points, comme nous le verrons au cours du chapitre 4. Toutefois, l'utilisation d'une identité numérique persistante est nécessaire pour qu'une relation de confiance puisse apparaître, ne serait-ce que par rapport à l'utilisation des systèmes de réputation. Tout l'enjeu des DNMs réside donc au sein de cette négociation permanente entre anonymat et pseudonymat.

Dans la partie qui suit, nous allons nous intéresser à la question de la confiance comme phénomène social, et de quelle manière la technologie a et continue de participer à l'évolution de cette notion.

10. Ma traduction. Citation originale : « An attribute is a characteristic associated with an entity, such as an individual. Examples of persistent attributes include eye color, and date of birth. Examples of temporary attributes include address, employer, and organizational role. A Social Security Number is an example of a long-lived attribute in the American governmental system. Passport numbers are long-lived attributes. »

11. Ma traduction. Citation originale : « Identity is that set of permanent or long-lived temporal attributes associated with an entity. »

12. Ma traduction. Citation originale : « An identifier distinguishes a distinct person, place or thing within the context of a specific namespace. [...] One person, place, or thing can have multiple identifiers. [...] Each identifier is meaningful only in the namespace, and only when associated with the thing being identified. »

13. Ma traduction. Citation originale : « An anonym is an authenticated attribute that is not linked to an identifier. An identifier associated with no personal identifier, but only with a single-use attestation of an attribute is an anonym. An anonymous identifier identifies an attribute, once. An anonymous identifier used more than once becomes a pseudonym. »

2 La notion de confiance

La confiance est une notion sociale que l'on utilise tous les jours, de manière instinctive, sans en saisir pourtant pleinement les enjeux et la signification. De nombreux auteurs se sont attelés à la tâche de la définir, et deux définitions nous sont utiles pour mieux comprendre comment la confiance s'inscrit dans les pratiques que l'on retrouve sur les DNMs :

La confiance est « un acte consistant à se rendre volontairement vulnérable aux actions d'autrui, en acceptant la possibilité que “les choses tournent mal” tout en entretenant la croyance que cela n'arrivera pas de façon vraiment grave. » (NOOTEBOOM, 2006, p. 65)

« Il peut être dit d'un individu qu'il a confiance en la réalisation d'un événement s'il s'attend à ce que ce dernier ait lieu et que son attente donne lieu à un comportement perçu comme ayant de plus fortes conséquences négatives si l'événement ne se produit pas que de conséquences positives si l'événement se produit. »¹ (DEUTSCH, 1958, p. 266)

Deux éléments centraux ressortent de ces définitions. Le premier est l'idée d'un comportement *volontaire*, lorsqu'un individu se rend vulnérable aux actions d'autrui. On pourrait pour saisir cette notion de volontariat donner l'argument que, dans la vie quotidienne, un individu fait en permanence confiance aux personnes qu'il croise au cours de sa journée. Il fait confiance aux automobilistes pour s'arrêter aux feux rouges et ne pas l'écraser quand il traverse la route, il fait confiance à son employeur pour que celui-ci lui verse le salaire convenu à la fin du mois, et ainsi de suite. D'après Luhmann (2006a), c'est pour cela qu'il est important de faire la distinction entre confiance *assurée* et confiance *décidée*.

La confiance assurée survient lorsque le fait de faire confiance nous est imposé. Ainsi, nous sommes tous obligés de faire confiance aux automobilistes pour ne pas nous écraser, sinon nous ne sortirions jamais de chez nous. En revanche, la confiance décidée survient après une action réfléchie de notre part, qui donne lieu à de potentielles conséquences négatives.

1. Ma traduction. Citation originale : « An individual may be said to have trust in the occurrence of an event if he expects its occurrence and his expectation leads to behaviour which he perceives to have greater negative motivational consequences if the expectation is not confirmed than positive motivational consequences if it is confirmed. »

La confiance décidée implique des calculs de « rentabilité de la confiance » (DEUTSCH, 1958), qui est le deuxième point central des définitions données plus haut. Pour pouvoir faire confiance, il faut que cette confiance puisse être trahie et que cette trahison ait des conséquences négatives. Un exemple souvent donné dans la littérature est celui du ou de la baby-sitter. Le ratio bénéfice/risque de l'engagement d'un.e baby-sitter semble en théorie bien trop négatif pour être rentable : le bénéfice est simplement pour le ou les parents de pouvoir passer une soirée entre adultes, alors que le risque potentiel est que le ou la baby-sitter fasse du mal à leur enfant. Néanmoins, chaque jour, des dizaines de milliers de baby sitter sont engagé.e.s à travers le monde sans que cela n'ait de conséquences négatives pour qui que ce soit.² Il en va de même pour les milliers de transactions réalisées sur les DNMs depuis l'avènement de Silk Road, comme discuté dans l'introduction de ce travail.

Finalement, quand nous décidons de faire confiance à autrui, nous choisissons également de faire comme si cette confiance ne pouvait pas être trahie. Le risque existe, nous le savons, mais nous ne le prenons pas en compte.

2.1 Son rôle dans les interactions

2.1.1 Mécanisme de réduction de la complexité sociale

Reprenons l'exemple donné plus haut, de la confiance envers les automobilistes qui respectent le code de la route, et généralisons le. Chaque individu, chaque institution, chaque entité dont nous croisons le chemin peut avoir un comportement qui nous est néfaste. Si nous réfléchissons à toutes les manières dont nous pourrions souffrir du comportement d'autrui, il nous serait *de facto* impossible d'agir. Chacun serait paralysé par l'angoisse, et la société dans son ensemble ne pourrait pas fonctionner (LUHMANN, 2006b). Hors, malgré cette situation de départ que l'on pourrait qualifier de hobbesienne, cela n'est pas le cas.

Ainsi, si la confiance augmente la complexité du système social, en augmentant le nombre de situations qu'elle peut réconcilier, elle diminue également la complexité du monde. Faire confiance à autrui nous offre un nombre de possibilités d'agir presque infini, mais celles-ci s'inscrivent toutes dans un cadre social particulier.

Néanmoins, ces possibilités infinies présentent un autre problème, bien défini par Lumann (ibid., p. 13) : « l'avenir contient un nombre beaucoup plus élevé de possibilités que celles qui peuvent être actualisées dans le présent et qui, de ce fait, peuvent être transférées dans le passé. [...] L'avenir surcharge le potentiel de présentification de l'être humain. Et pourtant, l'humain doit vivre dans le présent avec un avenir toujours

2. Rachel Botsman (2017) consacre un chapitre de son livre à l'étude du site UrbanSitter, et le parallèle avec les DNMs est flagrant : des inconnus sont mis en relation par une plateforme Internet, dans une interaction qui peut avoir des conséquences catastrophiques pour l'une des deux parties si elle se passe mal, et les systèmes d'évaluation et de réputation font le cœur de la plateforme.

hypercomplexe. Il doit donc constamment découper son futur à l'aune de son présent, c'est à-dire réduire la complexité. ». En d'autres termes, nous vivons dans un dilemme du prisonnier permanent. Avant d'agir, nous devons savoir comment les autres vont probablement agir. Mais eux aussi doivent savoir comment nous comptons agir, et ainsi de suite.

La conséquence de cet avenir hypercomplexe est que nous devons constamment manipuler le présent d'autrui pour que nos avenir coïncident. Cette manipulation, nous le verrons plus bas, peut prendre plusieurs formes, mais doit toujours se réaliser de manière subtile. Si l'on manipule le présent des autres de manière trop évidente, la confiance laisse en effet la place au soupçon. Notre interlocuteur commence alors à se poser la question de nos intentions véritables, et à ce que l'on pourrait potentiellement cacher.

Pour que la confiance puisse pleinement jouer son rôle de mécanisme de réduction de la complexité sociale, elle doit ainsi pouvoir cohabiter avec le soupçon, mais sous une forme qui l'immunise contre lui.

2.1.2 Le problème de la double contingence

Si le monde social est si complexe, c'est non seulement en raison des possibilités infinies que nous offre l'avenir, mais également en raison d'un concept développé par Scott Parsons (1968) : la double contingence. Ce concept soulève la question de comment deux individus qui se trouvent en situation d'interaction arrivent à combler le vide qui les sépare et à établir une relation. Au cours de l'interaction, qui implique un *alter* et un *ego*, comment est-ce que la réorganisation de l'*alter* influence *ego* ? Et comment est-il possible de coordonner des actions entre *alter* et *ego* ?

Cette question génère un problème au niveau social, qui a besoin d'une solution afin qu'interactions sociales et ordre social puissent s'établir. Pour Parsons, cette solution existe sous la forme d'un « système de symboles partagés » (VANDERSTRAETEN, 2002, p. 81), c'est à dire d'intersubjectivité. La position de Parsons est la suivante : quand *ego* réalise une action élémentaire envers *alter*, il s'engage dans un processus de symbolisation. *Ego* met en jeu une attente, qui implique alors nécessairement une généralisation issue des spécificités de la situation. *Alter* réagit à *ego* en contingence à la proposition de ce dernier : il articule également ses attentes, et s'engage ce faisant dans une nouvelle étape de symbolisation.

Deux acteurs ayant déjà acquis un système de symboles agissent et réagissent de manière particulière dans des situations spécifiques, de telle sorte qu'ils activent des formes culturelles relativement stables, et plus ou moins partagées. Celles-ci donnent alors à la situation un sens suffisamment généralisé pour laisser apparaître la possibilité de la communication.

Pour simplifier, si deux individus souhaitent pouvoir établir une interaction, ils doivent auparavant trouver un plus petit dénominateur commun issu de la situation spécifique dans laquelle ils se trouvent. Sur les DNMs par exemple, les situations peuvent paraître très spécifiques : deux individus anonymes utilisent des technologies complexes afin de s'échanger des substances illicites contre des cryptomonnaies. Mais, fondamentalement, cette interaction se résume à une transaction commerciale que chacun a déjà vécue de nombreuses fois. Les acteurs font finalement abstraction de toutes les particularités de la situation pour ne se concentrer que sur les généralités communes qui existent entre eux. Pour cette raison, la confiance est un raisonnement qui va du psychologique (raisonner de soi aux autres) vers le totalement sociologique (généraliser à partir des expériences d'autrui) : « Si je peux honorer la confiance placée en moi par un absolu inconnu, alors je peux moi aussi faire confiance à des inconnus » (SHEETS-JOHNSTONE, 2006, p. 29).

En étant à la fois un moyen de diminuer la complexité du monde social et de régler le problème de la double contingence, on comprend alors mieux l'importance de la confiance comme point de passage obligé sur le darknet. Mais, en étant un PPO, la confiance fait aussi « peser sur les individus, agents ou destinataires, des charges élevées : c'est pour cela qu'elle représente un lien qu'il faut réactiver en permanence – comme aujourd'hui dans les communautés minoritaires, les groupes criminels, les réseaux et les organisations secrètes où il faut, entre soi, multiplier et ritualiser les signes d'appartenance et de fiabilité, les gestes et les postures qui signifient qu'on peut compter les uns sur les autres » (Stéphane HABER, 2006, p. 53). C'est également pour cela, comme nous allons le voir au cours du chapitre 3, que les opérations les plus efficaces de la part des forces de police sont celles qui mettent à mal les relations de confiance plutôt que celles qui visent des individus isolés.

2.2 Confiance et nouvelles technologies

Les nouvelles technologies de l'information et de la communication (NTIC) sont aujourd'hui présentes dans tous les domaines de la vie quotidienne. La confiance étant, on vient de le voir, compliquée à mettre en place et difficile à maintenir, il est normal d'assister à l'émergence de technologies supposées servir de cadre à sa mise en place.

2.2.1 Modalisation de la confiance à travers les NTIC

Suite à la crise de 2008, la confiance du public envers les institutions étatiques diminua fortement. Un indice de cette baisse se trouve dans les résultats du *Gallup Poll*,³ dont les indicateurs en matière de confiance n'ont jamais été aussi bas (BOTSMAN, 2017).

3. Le *Gallup Poll* est un sondage réalisé à travers le monde depuis 1935 par l'entreprise Gallup. Il mesure les attitudes des citoyens de plus de 130 pays à propos de nombreuses problématiques. Définition tirée de <https://goo.gl/vvjYww>, accédé le 30.07.2018

En 1935, 75% des citoyens américains déclaraient avoir « a great deal or a fair amount of trust and confidence » envers le gouvernement fédéral pour régler les problèmes internationaux, et en 2016 la confiance moyenne envers 14 institutions américaines était de 32% en moyenne.

Si les individus ne font plus confiance aux institutions, gouvernementales ou privées, leur confiance s'est reportée sur les citoyens ordinaires : « les gens ont plus de chance de décrire “une personne comme moi” comme source d'information crédible. Un ami, voire un ami sur Facebook, est aujourd'hui vu comme deux fois plus digne de confiance qu'un chef de gouvernement, d'après le Edelman Trust Barometer »⁴ (ibid., p. 47).

Cette augmentation de la confiance envers “une personne comme moi” s'est traduite par le succès, au cours des dernières années, des dispositifs visant à agglomérer, sur Internet, les avis des consommateurs pour tout et n'importe quoi. Il est aujourd'hui possible de donner son avis à propos d'une « très grande diversité de biens et services : cosmétiques, hôtels et restaurants, électroménager, appareils photos, mais aussi garagistes, pompes funèbres, services bancaires, etc. » (BEAUVISAGE, BEUSCART, CARDON et al., 2013, p. 133). L'idée est ici que la moyenne des avis d'une grande masse d'individus sera plus fiable que celle de quelques experts. Nous étudierons cette question plus en détail au cours du chapitre 4, mais celle-ci permet de donner une piste de réponse à propos du succès des DNMs. Les expériences offertes aux utilisateurs de ces plateformes ne sont pas totalement nouvelles, et ne sont que la *modalisation* (GOFFMAN, 1974) de pratiques déjà existantes ailleurs sur Internet.

Néanmoins, le facteur humain est toujours présent au cœur de ces pratiques, et cela met à mal cette velléité de confiance absolue que l'on pourrait porter à ces NTIC. Aujourd'hui, le but vers lequel tendent ces technologies est d'avoir des systèmes purement automatisés, réduisant autant que faire se peut l'erreur humaine, ou tout simplement les possibilités de nuisance d'agents mal intentionnés.

L'exemple de la blockchain

La blockchain est un exemple concret de cette philosophie de « gouvernementalité algorithmique » (ROUVROY et BERNIS, 2013). Le concept en tant que tel date d'il y a quelques décennies (pour sa première présentation, voir Stuart HABER et STORNETTA, 1990), mais son application dans le monde réel a vu le jour à partir de 2008 avec la mise en place du système de minage de bitcoins (NAKAMOTO, 2008).

Cette cryptomonnaie fonctionne en utilisant le principe suivant : des mineurs minent des “blocs” numériques en résolvant des opérations mathématiques de plus en plus complexes. Lorsqu'un bloc est miné, le mineur ou le groupe de mineurs ayant résolu l'opération mathématique gagne une récompense fixe en BTC, récompense divisée par

4. Ma traduction. Citation originale : « People are more likely to describe “a person like me” as the most credible source of information. A friend, or, say, a Facebook friend, is now viewed as twice as credible as a government leader, according to the Edelman Trust Barometer. »

deux tous les 210.000 blocs.⁵ Au sein de ce bloc, un certain nombre de transactions en BTC peuvent être inscrites. Une fois inscrite, une transaction est validée lorsque le bloc est miné, et le bloc qui vient d'être miné est ajouté à la liste de tous les autres blocs minés précédemment. De plus, le bloc situé en position n dans la blockchain contient en son sein une référence vers le bloc $n-1$. Ainsi, tous les blocs sont liés par leurs références mutuelles, et les transactions qui y sont inscrites le sont de manière publique et permanente. D'où le nom donné à la blockchain de "livre de comptabilité public".⁶

Nous reviendrons plus bas sur les failles inhérentes à ce système, mais le fait est qu'aujourd'hui la blockchain est une mise en pratique de cette volonté d'encadrer les pratiques humaines par des technologies "fiables et objectives". Pourquoi prendre le risque de faire confiance à des êtres humains lorsque l'on peut s'en remettre à un algorithme ?

2.2.2 La *digital trust* : une utopie ?

Nous l'avons vu plus haut, la confiance est plus compliquée à instaurer et à conserver dans un cadre réticulaire que dans le cas d'une interaction sociale en face à face. Le nombre d'entités à prendre en compte, ainsi que l'absence du corps physique d'autrui rendent nécessaire de faire des suppositions : « most current digital systems are designed based on the assumptions that the user trusts his/her device fully ; or the user has to trust a service provider. » (YAN et HOLTSMANN, 2008, p. 15).

Les NTIC ont donc un rôle important à jouer en matière de confiance digitale : la confiance étant le produit des expériences passées et de la confiance perçue, leur but est d'augmenter la confiance perçue de manière significative, notamment envers les plateformes au sein desquelles se déroulent les interactions. Il paraît compliqué à première vue de faire confiance à un vendeur sur un DNM en lui transmettant ses informations personnelles (nom et prénom, adresse), mais s'il apparaît sur le site que des milliers de personnes ont sauté le pas avant nous, il sera plus facile de le sauter également.

Là où les NTIC sont utilisées, elle doivent toutefois négocier leur rôle en permanence. Yan et Holtmann (ibid.) mettent ainsi l'accent sur la différence entre *soft trust* et *hard trust* : la *soft trust* est le fait de faire confiance en se basant sur des critères subjectifs propres à chacun, alors que le *hard trust* est la confiance envers des critères objectifs. Sur les DNMs il pourrait s'agir du nombre brut d'évaluations reçues par un vendeur, sans s'intéresser à leur contenu. La *soft trust* pourrait alors se baser sur des critères tels que la manière dont un vendeur rédige son profil ou présente ses produits.

5. C'est que l'on appelle le *halving*.

6. *Public ledger* en anglais.

Si la confiance est induite de manière trop flagrante par la technologie, celle-ci perd son rôle facilitateur et devient même un obstacle à son apparition : « l’agir sur l’expérience duquel la confiance s’appuie doit apparaître comme étant l’expression de la personnalité et il doit confirmer celle-ci. Une action ne lui sera attribuée que si elle est institutionnalisée comme étant “libre” » (LUHMANN, 2006b, p. 46). Comment dans ce cas considérer les évaluations laissées par les autres utilisateurs, lorsque sur les DNM s il est obligatoire d’en laisser une pour finaliser une transaction ? D’autant plus que l’évaluation est par défaut positive, avec une note de 5/5 sur les différents critères proposés. C’est ce que montre la figure 2.1, capture d’écran de l’interface d’évaluation du marché Darknet Heroes League (DHL).⁷

FIGURE 2.1 – L’interface d’évaluation sur DHL

L’émergence de la notion de confiance digitale s’est faite aux dépens de celle de supererogatoire : « une opération est supererogative lorsque, sans correspondre à un devoir, elle est considérée comme un mérite et force le respect » (ibid., p. 49). La fonction du supererogatoire est de transformer les conditions d’émergence en conditions de la conservation, et s’oppose finalement à celle des NTIC, qui ne se focalisent que sur les conditions d’émergence.

Cette mauvaise compréhension de la part des partisans des NTIC explique à elle seule les “crises” de la confiance qu’ont traversé certains sites. Citons notamment AliBaba, qui dut faire face en 2011 à une polémique lorsqu’il fut révélé que des employés de l’entreprise avaient travaillé de concert avec certains vendeurs frauduleux pour leur offrir un badge *Assessed Supplier* qu’ils ne méritaient pas.⁸

Pour conclure cette partie, nous pouvons affirmer que la *digital trust* n’est pas une utopie, puisqu’elle permet l’apparition de relations et d’échanges commerciaux qui n’auraient pas pu voir le jour sans elle. C’est une notion dont la définition reste néanmoins floue,⁹ et qui donne lieu à des situations non optimales en matière de

7. Cette pratique de mettre par défaut la note maximale se retrouve sur la plupart des marchés actuels, et pas seulement sur DHL.

8. <https://goo.gl/Cm1ZQF>, accédé le 30.07.2018

9. Même si cela est sans doute dû à la récence de son apparition dans l’espace public.

pratiques sociales en ligne : « online peer-to-peer communities involve inherently political dimensions, which cannot be dealt purely on the basis of protocols and algorithms. » (DE FILIPPI et LOVELUCK, 2016, p. 2).

3 Darknet & *marketplaces*

3.1 Historique

Bien que l'on puisse considérer que l'achat et la vente de substances illicite sur Internet aient vraiment explosé aux alentours de 2006, ce genre d'échange était possible bien avant cette date. Au début des années 1970 par exemple, des étudiants de Stanford utilisèrent ARPANET, l'ancêtre d'Internet, pour acheter du cannabis à des étudiants du MIT (MARKOFF, 2005). La transaction ne se fit pas sur Internet, le réseau dans ce cas précis ne servant qu'à mettre acheteurs et vendeurs en contact. Toujours est-il que, des années avant que le public ne puisse acheter des biens et des services en ligne, le réseau était déjà utilisé pour se procurer de la drogue.

Usenet, que l'on pourrait considérer comme l'ancêtre des forums modernes, était administré au cours des années 80 par la *backbone cabal*, un groupe de personnes responsables du bon déroulement des opérations sur les *newsgroups*¹ et du maintien de l'ordre sur la plateforme. En 1987, John Gilmore et Brian Reid créèrent le *newsgroup alt*, pour échapper à la censure des administrateurs, alors considérés comme trop puritains. En avril 1988, Brian Reid leur envoya le mail suivant :

Pour mettre fin au suspense, je viens de créer alt.sex. Ce qui veut dire que le réseau alt comporte maintenant alt.sex et alt.drugs. Il était donc artistiquement nécessaire de créer alt.rock-n-roll, ce que j'ai également fait. Je n'ai aucune idée de la fréquentation que cela va entraîner. Si les bizarroïdes l'envahissent je compte le rmgroup² ou le modérer. Sinon, je le laisserai exister.

Brian Reid³

De la même manière que les étudiants du MIT et de Stanford, les participants à alt.drugs ne pouvaient pas se servir du réseau pour échanger directement de l'argent, les technologies n'existant à l'époque tout simplement pas. Le *newsgroup* servait simplement de point de rencontre entre offre et demande. D'autres forums dédiés à ces pratiques continuèrent d'apparaître toute la fin du XX^{ème} et le début du XXI^{ème}

1. Usenet est organisé autour du principe de groupes de discussion ou groupes de nouvelles (en anglais *newsgroups*), qui rassemblent chacun des articles (contributions) sur un sujet précis. (Wikipédia)

2. La commande `rmgroup` est utilisée pour supprimer un *newsgroup*.

3. Ma traduction. La citation originale est visible ici : <https://goo.gl/PfWTs1>

siècle, mais c'est en 2006 que les DNMs tels que nous les connaissons émergèrent pour de bon, avec la création de Adamsflower.

Ce site, lancé en 2006, était un marché en ligne qui permettait à des vendeurs de vendre directement depuis la plateforme moyennant le paiement d'une commission. Le site ne disposant pas de système de chiffrement intégré, les utilisateurs échangeaient via Hushmail, un fournisseur de mails permettant de chiffrer ses communications.⁴ Pour des raisons de sécurité et d'ergonomie, le site migra sur Tor en 2010, et prit le nom de The Farmer's Market (TFM).

Le site resta en ligne jusqu'au début de l'année 2012, date où ses fondateurs furent arrêtés. Des agents américains avaient infiltré le marché en se faisant passer pour des clients, et suivi des transactions à la trace pour remonter jusqu'aux administrateurs. Sans moyen de réaliser des transactions financières de manière anonyme, les utilisateurs du site devaient utiliser PayPal ou Western Union, ce qui facilita grandement la tâche des forces de l'ordre.

Nous venons de le voir, si les DNMs modernes ne sont apparus que récemment, les pratiques qui ont lieu dessus précèdent en réalité Internet tel que nous le connaissons aujourd'hui. Il faudra toutefois attendre l'apparition de certaines technologies, ainsi que l'atteinte d'une masse critique d'utilisateurs, pour que les DNMs deviennent le phénomène qu'ils sont actuellement.

3.1.1 Silk Road

Lancement du marché et arrestation de son créateur

Silk Road peut être considéré comme le premier DNM moderne, intégrant dans son fonctionnement la plupart des technologies nécessaires à la bonne marche d'un marché :

- Hébergement sur Tor
- Système d'*escrow*⁵
- Paiement en bitcoins

Lancé en février 2011, le marché était à ses débuts assez confidentiel, et comptait un nombre restreint d'utilisateurs ainsi que de listings. Suite à un article paru dans la presse en juin 2011,⁶ son activité explosa (BEARMAN, 2015). L'article donnait en effet aux lecteurs l'URL du site ainsi que le moyen d'y accéder, ce qui était auparavant destiné à un public d'initiés.

Un effet de l'engouement provoqué par l'article est visible lorsque l'on s'intéresse au cours du BTC pour l'année 2011, montré figure 3.1. Même s'il est compliqué

4. <https://goo.gl/EhAFHY>, accédé le 17.07.2018

5. Nous reviendrons sur ce concept au cours du chapitre 4

6. <https://goo.gl/bBJgvJ>, accédé le 20.07.2018

de prouver que cette hausse du cours fut effectivement liée à l'augmentation de la demande en BTC afin d'acheter des produits sur le marché, la cryptomonnaie perdit 25% de sa valeur quelques années plus tard lorsque le marché fut mis hors ligne par le gouvernement américain.



FIGURE 3.1 – Le cours du BTC, en dollars américains, de janvier à juillet 2011.⁷

Suite à cet article, l'attention des pouvoirs publics américains se tourna vers le marché, et ceux-ci mirent en place l'opération Marco Polo afin d'arrêter la ou les personnes responsables du fonctionnement de la plateforme. L'opération impliquait le FBI, la DEA,⁸ le DHS,⁹ l'IRS,¹⁰ le service secret américain, et l'ATF.¹¹



FIGURE 3.2 – La page d'accueil de Silk Road suite au succès de l'opération Marco Polo.¹²

7. Obtenu à partir de <https://goo.gl/qLSFjT>

8. Drug Enforcement Administration, l'agence américaine chargée de la lutte contre la drogue.

9. Department of Homeland Security, l'équivalent américain du ministère de l'intérieur.

10. Internal Revenue Service, le fisc américain.

11. Bureau of Alcohol, Tobacco, Firearms and Explosives, agence fédérale américaine chargée de tout ce qui concerne l'alcool, le tabac, les armes à feu et les explosifs.

12. Du Federal Bureau of Investigation - <https://goo.gl/MD5jzN>, Domaine Public, <https://goo.gl/jjrCnC>

L'opération porta ses fruits, et Ross Ulbricht fut arrêté quelques mois après le début de la traque, alors qu'il était connecté sur l'interface d'administration de Silk Road, sous le pseudonyme Dread Pirate Roberts (DPR) (BEARMAN, 2015). Il fut condamné à une double peine de prison à vie sans possibilité de libération sur parole, à laquelle vint s'ajouter une peine de 40 ans de prison.¹³ Son arrestation sonna le glas des activités de Silk Road, dont la page d'accueil fut remplacée par un message du gouvernement américain, visible figure 3.2.

L'identité *Dread Pirate Roberts*

Dans le cadre de ce travail, l'arrestation de Ross Ulbricht est riche en leçons.

Dread Pirate Roberts est un personnage du film *The Princess Bride*, sorti en 1987. Pirate à la réputation internationale, il n'est en réalité pas un individu, mais une suite de personnes se transmettant le nom une fois qu'ils sont suffisamment riches pour ne plus exercer cette activité. Nous entrons ici dans le domaine de la conjecture, mais en partant du principe que ce pseudonyme a été choisi avec soin, nous pourrions tout à fait imaginer que Silk Road ait été administré par plusieurs personnes, chacune se connectant avec le même compte.

Nous avons vu plus haut les définitions de différentes notions : identité et identité numérique, identifiant et attribut, etc. L'arrestation de Ross Ulbricht met en exergue l'importance de séparer autant que possible identité civile et numérique, notamment en n'utilisant que certains attributs dans un « espace de noms » (CAMP, 2004) donné, et d'autres dans un autre.

Le fondateur de Silk Road demanda par exemple de l'aide sur StackOverflow, un forum d'entraide pour programmeurs, en utilisant son vrai nom. Se rendant compte de son erreur, il changea très vite son pseudonyme pour *frosty*.¹⁴ Ce pseudonyme fut ensuite réutilisé dans les clefs de chiffrement des serveurs du marché.

Ross Ulbricht → *frosty* ← **Silk Road**

FIGURE 3.3 – *frosty*, lien entre Ross Ulbricht et Silk Road

L'erreur de *frosty* fut d'utiliser ce pseudonyme dans un espace de noms pouvant être à la fois relié à Ross Ulbricht et à Silk Road.

En utilisant le pseudonyme *altoid*, Ross Ulbricht ouvrit également un sujet sur le forum Bitcointalk, dans lequel il annonçait chercher à recruter un professionnel de l'informatique pour travailler avec lui sur un projet de startup dans le domaine des bitcoins.¹⁵ Les personnes intéressées par l'annonce étaient invitées à lui répondre en envoyant un e-mail à l'adresse `rossulbricht@gmail.com`.

13. <https://goo.gl/45SJUK>, accédé le 20.06.2018

14. La question est toujours visible : <https://goo.gl/Wv3sGu>, accédé le 20.07.2018

15. Le sujet est toujours visible : <https://goo.gl/zSp5Y6>, accédé le 20.07.2018

De nombreuses autres traces furent laissés çà et là par Ross Ulbricht, qui furent ensuite utilisés par le gouvernement américain comme des “alliés” dans la création du lien qui reliait le définitivement au cours du procès à Silk Road. Ce lien joua le rôle d’une « boîte noire » lors de sa condamnation, que Ross Ulbricht ne pouvait plus déconstruire tellement elle comportait d’éléments différents. Chacun de ces éléments pris séparément n’aurait eu que très peu de poids dans la construction du lien, et cela confirme la définition d’une identité numérique comme un ensemble d’informations et de traces (LECOMTE, 2010).

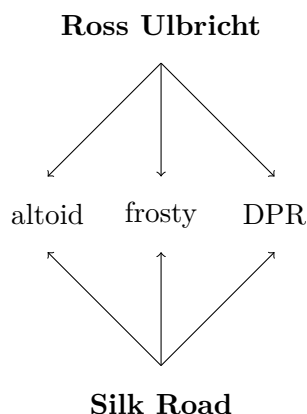


FIGURE 3.4 – Le faisceau des liens reliant Ross Ulbricht à Silk Road

3.1.2 L’âge d’or des DNMs

La période post Silk Road

La mise hors ligne de Silk Road n’eut pas l’effet escompté. Fortement médiatisé, l’événement montra à quel point l’administration d’un DNM pouvait être profitable : l’ordinateur de Ross Ulbricht contenait 144.000 BTC au moment de son arrestation (BEARMAN, 2015), soit plus de 20 millions de dollars en considérant un cours de 150\$/BTC en octobre 2013.

A partir d’octobre 2013, de nouveaux DNMs arrivèrent régulièrement sur le marché, notamment Silk Road 2.0, contrôlé par d’anciens administrateurs de Silk Road, ou encore Agora.¹⁶ Tous les DNMs lancés à cette époque ne connurent pas le succès de Silk Road, loin de là, et certains d’entre eux eurent des durées de vie se comptant en jours : Utopia ou CannabisRoad en sont des exemples.

L’amateurisme de la plupart des équipes contrôlant ces nouveaux DNMs les conduisit à commettre de nombreuses erreurs, et en novembre 2014 les gouvernements de 17 pays déclenchèrent l’*Operation Onymous*, mettant hors ligne 27 sites cachés, dont 14

¹⁶. Ce DNM resta en ligne durant presque deux ans, de fin 2013 à août 2015, et fut l’un des seuls DNMs à arrêter ses opérations sans *exit scam* ou sans que ses administrateurs ne soient arrêtés.

étaient des DNMs. Silk Road 2.0 fut saisi,¹⁷ ainsi qu'Alpaca, Black Market, Cloud Nine, etc.¹⁸

Quelques plateformes ne furent pas impactées par cette opération, Evolution et Agora devenant alors respectivement le premier et deuxième plus importants DNMs de l'époque.

Disruption de la confiance

Les forces de l'ordre ayant montré qu'elles avaient un fort intérêt pour les DNMs, les techniques s'améliorèrent, les erreurs diminuèrent, et les opérations reprirent sans événement majeur. Si des vendeurs ou des acheteurs continuaient régulièrement de se faire arrêter, les marchés tinrent bon et Agora et Evolution confortèrent leurs positions de leaders.

En mars 2015, les administrateurs d'Evolution disparurent dans l'un des plus gros *exit scam*¹⁹ de l'histoire des DNMs, emportant avec eux 12 millions de dollars. Les utilisateurs du marché se répartirent alors sur ceux déjà existants, notamment Agora et Black Bank. En avril 2015, Agora était le plus gros DNM ayant jamais existé, et comptait plus de listings que Silk Road à son apogée.²⁰

Black Bank disparut à son tour dans un *exit scam* en mai 2015, ce qui mena les utilisateurs à remettre en question la centralité des DNMs. Jusqu'à présent, il était en effet obligatoire de faire confiance à un marché pour pouvoir l'utiliser : le système d'*escrow* notamment, que nous verrons plus tard, force les utilisateurs à laisser le contrôle de leurs bitcoins à la plateforme, pouvant potentiellement mener à des *exit scams*. De plus, les serveurs des DNMs étant physiquement localisables, cela les rend vulnérable à des opérations telles que *Operation Onymous*. De nouvelles techniques telles que le multi-sig virent le jour, et Open Bazaar, un marché distribué sur les machines des utilisateurs, fut mis en ligne en avril 2016.

Ces nouvelles pratiques ne furent néanmoins pas adoptées par la majorité des utilisateurs, et les DNMs centralisés continuèrent de prospérer malgré les failles devenues saillantes au cours des derniers mois.

17. Silk Road 3.0 vit le jour quelques heures seulement après la saisie des serveurs de Silk Road 2.0.

18. La liste complète est disponible ici : <https://goo.gl/goJbR9>, accédé le 20.07.2018

19. Un *exit scam* est le fait pour un DNM ou un vendeur de disparaître avec l'argent des utilisateurs. Dans le cas d'un vendeur, cela consiste à ne pas honorer les dernières commandes, et dans le cas d'un DNM il s'agit d'interrompre la possibilité de retirer l'argent du marché, de la même manière qu'une banque pourrait empêcher ses clients d'accéder à leurs comptes.

20. <https://goo.gl/uPy5w8>, accédé le 20.07.2018

3.2 *Operation Bayonet et ses conséquences*

En octobre 2015, AlphaBay était le marché comptant le plus de listings dans l'écosystème des DNMs. Hormis un *exit scam* de la part de Nucleus en avril 2016, cette période peut être considérée comme une période de relative tranquillité, les marchés disparaissant à cette époque n'étant pas suffisamment centraux pour que cela ait un impact significatif sur les pratiques.

3.2.1 La destruction du PPO

C'est en juillet 2017 que les forces de l'ordre portèrent un coup presque fatal à la confiance des utilisateurs envers vendeurs et DNMs. Si jusque là les différentes opérations consistaient à saisir des serveurs et à arrêter des administrateurs, *Operation Bayonet* montra à quel point le PPO explicité plus haut jouait un rôle central.

Arrestation d'Alexandre Cazes et disparition d'AlphaBay

En juin 2017, AlphaBay comptait 369.000 listings pour 400.000 utilisateurs²¹, soit une taille 10 fois supérieure à celle de Silk Road. Le marché était géré par Alexandre Cazes, qui avait commis les mêmes erreurs de Ross Ulbricht en créant la plateforme :

- Utilisation de sa véritable adresse e-mail lors de l'envoi de messages de bienvenue suite à l'inscription sur le site
- Réutilisation d'un pseudonyme associé à son identité pour promouvoir le marché
- Hébergement des serveurs via une société à laquelle il avait fourni sa véritable identité
- Absence de chiffrement sur l'ordinateur portable servant à administrer le site

Celui-ci fut arrêté dans le cadre de l'*Operation Bayonet* le 5 juillet 2017 à Bangkok, les serveurs du marché saisis, et la page d'accueil remplacée par la capture d'écran de la figure 3.5.

Transformation de Hansa en *honeypot*

Hansa, qui était à l'époque le deuxième DNM en terme de taille, vit son nombre d'utilisateurs exploser. Acheteurs et vendeurs étaient coutumiers de ce genre de disparition, et hormis quelques pertes financières pour les plus malchanceux, les conséquences d'une saisie étaient moindres. Le *business as usual* reprit, jusqu'au 20 juillet 2017.

21. <https://goo.gl/JPqowF>, accédé le 20.07.2018



FIGURE 3.5 – La page d’accueil d’AlphaBay après Operation Bayonet

C’est à cette date que la véritable nature de l’opération fut révélée, lorsqu’il fut annoncé que le DNM était tombé entre les mains de la justice le 20 juin, sans qu’aucune annonce ne fut faite. Les responsables de l’opération avaient profité de ces quelques semaines pour apporter des modifications au marché, en sachant qu’avec la disparition prochaine d’AlphaBay celui-ci connaîtrait un influx important de nouveaux membres :

- Modification de la fonction d’auto chiffrement via PGP pour correspondre à une clef privée contrôlée par la *taskforce* responsable de l’opération, qui put alors déchiffrer les messages échangés par les utilisateurs, et contenant souvent les adresses des clients.
- Désactivation de la suppression automatique des métadonnées des photos importées sur le site, donnant accès à la police à des informations telles que la géolocalisation de chaque photo. Sous prétexte d’un “bug”, la police avait supprimé toutes les photos présentes sur le site pour pousser les vendeurs à les importer de nouveau.
- Modification des transactions en bitcoin utilisant le multi-sig, pour permettre la récupération des bitcoins une fois le site fermé.
- Les utilisateurs du site étaient également poussés à télécharger un fichier Excel, déguisé en fichier texte, contenant une macro permettant d’envoyer la véritable adresse IP de la machine sur un serveur web contrôlé par la police.

Toutes ces mesures permirent l’obtention des données privées d’un grand nombre d’acheteurs, et les responsables de l’opération annoncèrent avoir envoyé des “intelligence packages” à un grand nombre de pays, afin de donner lieu à des enquêtes concernant les acheteurs des pays concernés.²²

Cette opération eut pour effet de faire prendre conscience aux utilisateurs des DNMs que la confiance, qui semblait être le point central du système, « ne [faisait] plus

22. <https://goo.gl/7Y8G3G>, accédé le 20.07.2018

qu'exprimer le sentiment tranquille que, en gros, si opaque et compliqué que ça paraisse, *ça [fonctionnait]* » (Stéphane HABER, 2006, p. 53).

AlphaBay et Hansa mis hors service, et les acheteurs ayant appris que ce dernier marché était devenu un *honeypot*²³ durant les quelques semaines qui précédèrent sa mise hors ligne, la problématisation telle que montrée figure 1.1 se modifia étape par étapes. En premier lieu, le PPO disparut purement et simplement (figure 3.6), et il devint impossible pour les acteurs de « compter les uns sur les autres » (ibid.).

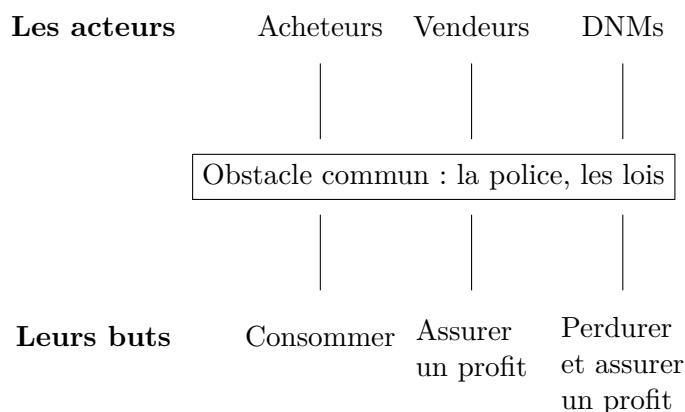


FIGURE 3.6 – Les DNMs sans PPO

Le message de l'utilisateur *hhayn* sur */r/DarknetMarkets* résume bien la situation, telle que vécue sur le moment par les différents acteurs :

« At this place point, who cares? Look at us for fuck sake. The uncertainty and lack of trust and really lack of community has allowed LE to break us. No one knows what the fuck is going on; markets are getting busted or disappearing or getting owned or being exposed; vendors are scamming to recoup losses from AB/Hansa; PGP keys are changing without warning; we got subterfuge and disinformation out the ass; buyers are scared of either getting busted in a lot of or honey or just getting burned; we have vigilantes pen testing markets for the safety of the community OR we have terrorist comen disrupting everything for their own benefit OR we have both.

I don't have the answers or solutions but I am also not giving up. Idk, I guess it is just frustration being vented. Shit went from being so simple (and taken for granted, to speak for myself), to a complete and utter nightmare. The more homework I do trying to figure the next moves, the fucking further away I become from the truth it feels like. »

Ce qu'acheteurs et vendeurs tenaient pour acquis était en réalité un équilibre instable, profondément perturbé par l'*Operation Bayonet*. Les conséquences s'en firent également

23. Dans le jargon de la sécurité informatique, *honeypot* (pot de miel) est une méthode de défense active qui consiste à attirer, sur des ressources (serveur, programme, service), des adversaires déclarés ou potentiels afin des les identifier et éventuellement les neutraliser (PASQUALE, 2015, p. 87).

ressentir pour les DNMs, qui durent gérer l'arrivée d'un nombre important de nouveaux membres, sans pour autant pouvoir répondre à leurs attentes. La figure 3.7 le montre bien, les admins de DHL disant que dans ce climat il leur était impossible d'engager qui que ce soit.



FIGURE 3.7 – La page d'accueil de DHL après *Operation Bayonet*.

3.2.2 Reconfiguration du schéma de problématisation

La force de cette opération fut de faire prendre conscience aux différents acteurs des DNMs que certains liens qui semblaient aller d'eux mêmes pouvaient en réalité être déconstruits, en particulier les liens entre les marchés et leurs membres. Hansa ayant été un *honeypot* pendant un mois, cela peut aujourd'hui potentiellement être le cas de n'importe quel DNM. Ceux-ci étant gérés anonymement, il est impossible pour acheteurs et vendeurs de savoir qui les opère réellement, et le risque existe qu'un utilisateur utilisant un marché plutôt qu'un autre soit en réalité en train de se faire piéger.

La demande pour des plateformes sur lesquelles échanger ne tomba toutefois pas à zéro, et de nombreux DNMs virent le jour durant cette période, afin de capter acheteurs et vendeurs. Cette situation de "ruée vers l'or" peut être problématisée à l'aide de la figure 3.8.

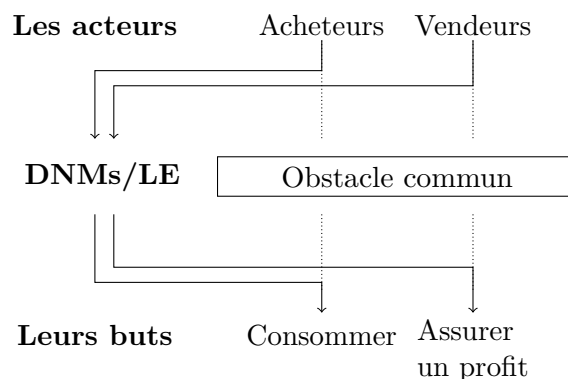


FIGURE 3.8 – Prise de conscience de la véritable configuration

Après l'*Operation Bayonet*, les marchés ne sont effectivement plus considérés comme des acteurs sur un pied d'égalité avec leurs membres, mais simplement comme un point de contact permettant à acheteurs et vendeurs de se rencontrer et d'échanger.

Ces points de contact pouvant également être contrôlés par LE,²⁴ il appartient aux membres de s'en éloigner le plus rapidement possible, ou tout du moins de sécuriser leurs pratiques afin de diminuer les informations transitant par les DNMs.

Perte exogène de la confiance

Ce que montre également cette opération, d'une manière postulée par Henslin (1968), c'est à quel point la source de la perte de confiance est importante. Après chaque *exit scam*, de la part d'un vendeur ou d'un marché, les pratiques n'ont que peu changé. En effet, il s'agissait là d'une attaque endogène, et seul l'auteur de l'*exit scam* était vu comme responsable. La confiance envers l'acteur individuel était perdue, mais persistait envers le système global.

L'*Operation Bayonet*, une attaque exogène envers le système, déstabilisa les fondements même de ce qui faisait que les DNMs fonctionnaient si bien jusqu'en 2017, tautologique au possible : les DNMs fonctionnaient simplement parce qu'ils avaient fonctionné, critère suffisant pour que les utilisateurs osent « effectuer un saut dans l'incertitude » (LUHMANN, 2006b). Après l'été 2017, les différents acteurs de cet écosystème durent revoir la manière dont ils utilisaient les ressources à leurs dispositions.

3.2.3 État des lieux

Étude de cas : TradeRoute et Aero

Aujourd'hui, un an après l'*Operation Bayonet*, le modèle des DNMs paraît être en déclin. Le risque est élevé pour les administrateurs de marché de tomber entre les mains de la justice un jour ou l'autre, ce qui donne aux marchés des durées de vie très limitées. L'exemple de Aero, visible figure 3.9 le montre bien.

Le lancement de ce marché se fit en octobre 2017, et fut l'occasion d'étudier le cycle de vie d'un DNM, de sa naissance à sa disparition. Étant donné le type de plateforme, on comprend aisément qu'il est impossible d'avoir accès à une API ou à des données publiques concernant l'utilisation du site. Ainsi, les seules observations possibles ont été limitées à ce qui était observable publiquement, c'est à dire le nombre de listings disponibles sur le marché.

Ce nombre évolua peu du 6 au 15 octobre, date à laquelle les administrateurs de TradeRoute, le gros marché du moment, décidèrent de réaliser un *exit scam*. Nous pouvons voir qu'à cette date, la courbe connaît une rapide croissance, jusqu'à arriver à un plateau vers le 23 octobre. À cette période, des attaques DDOS envers le marché rendaient son utilisation compliquée, et on peut imaginer que les vendeurs avaient du mal à s'inscrire et mettre des produits en vente. La croissance put reprendre après

24. *Law Enforcement*, les forces de l'ordre.

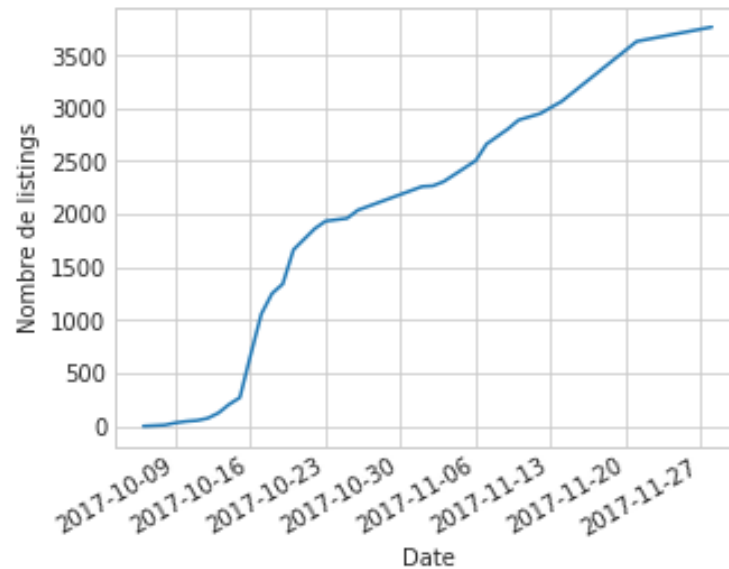


FIGURE 3.9 – Evolution du nombre de listings sur Aero

les attaques DDOS, même si elle ne fut jamais aussi rapide qu’après la disparition de TradeRoute. Les observations s’arrêtent fin novembre, au moment où Aero disparut à son tour dans un *exit scam*.

L’hypothèse que nous pouvons émettre suite à cette série d’observations est que, les conditions de survie d’un marché dans l’écosystème des DNMs étant bien plus strictes que quelques années en arrière, l’intérêt pour les administrateurs n’est plus de perdurer, mais de croître aussi vite que possible, amasser des BTC via le système d’*escrow*, puis de disparaître.

Il est évident qu’une seule série d’observations ne suffit pas pour généraliser à tous les DNMs, mais les observations d’un rapport publié en 2018 vont en faveur de cette hypothèse : « almost one year since the AlphaBay and Hansa takedowns, no single marketplace has risen to the top » (HOLLAND, AMADO et MARRIOTT, 2018, p. 4).

Les plateformes actuelles

Un petit nombre de DNMs sont aujourd’hui encore actifs, le plus gros d’entre eux étant Dream Market. Concernant ce dernier, la question de sa gestion se pose. En effet, comme le dit l’utilisateur *Ozaki8*, sur le forum du DNM Olympus, ayant eu lui aussi une courte durée de vie : « Dream est un marché zombie. Le corps est bien vivant, mais l’esprit est mort et porté disparu » (ibid., p. 5). Les administrateurs du marché ne communiquent sur aucune des plateformes à leur disposition, et habituellement utilisées par les équipes de relations publiques des marchés pour ce genre de communications. Il est alors possible que les administrateurs aient été arrêtés pour un crime sans lien avec les DNMs, et que le marché continue de fonctionner de manière automatique.

L'avantage de cette hypothèse est que l'erreur humaine est à présent impossible, et que le marché peut potentiellement fonctionner encore longtemps.

Quant à l'émergence de nouveaux marchés, elle semble aujourd'hui compromise pour plusieurs raisons. La première est que les clients potentiels craignent les *exit scams*, les *honeypots* et les mauvais vendeurs, et réussir à s'imposer comme un marché de confiance n'est pas chose simple.

La seconde raison concerne les coûts financier liés à la gestion et à l'administration d'un DNM. Le modèle économique de ces plateformes est classique, et consiste à prélever une taxe sur chaque vente. Ainsi, un DNM ayant énormément d'acheteurs aura un chiffre d'affaire suffisant pour payer les frais liés à une protection contre les DDOS, offrir un salaire aux administrateurs et développeurs, des récompenses aux hackers *white hat*,²⁵ et à tout de même réussir à dégager un profit valant la peine de prendre un tel risque. Hors, un marché se lançant aujourd'hui ne disposera pas d'une centralité suffisante pour atteindre un tel objectif étant donné les acteurs déjà présents.

La tendance actuelle consiste donc à la décentralisation totale des marchés, ceux-ci ne courant par définition pas le risque d'être mis hors ligne. La plateforme OpenBazaar notamment,²⁶ qui compte aujourd'hui un peu plus de 10.000 utilisateurs, fonctionne selon ce principe. Celle-ci ne proposant toutefois pas que des produits illicites, il est compliqué de connaître la proportion d'utilisateurs qui s'en servent comme d'un DNM. Quoiqu'il en soit, même en imaginant que les 10.000 individus présents sur OpenBazaar l'utilisent pour se procurer des substances, c'est un nombre bien faible comparé aux 400.000 utilisateurs inscrits sur AlphaBay à son apogée.

25. Un *white hat* (en français : "chapeau blanc ") est un hacker éthique ou un expert en sécurité informatique qui réalise des tests d'intrusion et d'autres méthodes de test afin d'assurer la sécurité des systèmes d'information d'une organisation. Par définition, les "white hats" avertissent les auteurs lors de la découverte de vulnérabilités. - Wikipédia

26. Accessible ici : <https://goo.gl/oMiYBa>

4 La création du lien de confiance sur les DNMs

Nous allons à présent nous intéresser à la manière dont il est possible de construire un lien de confiance sur les DNMs. Bien que la période pouvant être considérée comme leur “âge d’or” ait pris fin avec *Operation Bayonet*, de nombreux utilisateurs s’en servent toujours quotidiennement afin d’obtenir les produits qu’ils recherchent. En nous intéressant à la notion de confiance digitale, développée plus haut, nous avons vu que tous les comportements humains ne pouvaient pas être encadrés par la technologie.

Au sein de tout marché, virtuel ou non, légal ou non, il existe la possibilité pour les vendeurs de vendre des produits de mauvaise qualité. Cette simple possibilité peut potentiellement faire disparaître le marché dans son entièreté si rien ne vient pénaliser ces vendeurs, ou tout le moins les empêcher de vendre leurs mauvais produits (AKERLOF, 1978). C’est pour cette raison que, sur les marchés classiques, des organismes de contrôle existent et permettent d’en interdire l’accès aux vendeurs peu consciencieux. La teneur même des DNMs fait que l’existence de ces organismes est prohibée. Quelles stratégies sont-elles mises en place pour éviter les “lemons”(ibid.), c’est à dire les marchandises de mauvaise qualité? Quelle est la raison qui fait qu’acheteurs et vendeurs osent se lancer dans une « performance initiale risquée » (LUHMANN, 2006b)?

Au sein des DNMs, la confiance est créée de deux manières : par les technologies employées, et par les pratiques des différents acteurs. Nous allons nous intéresser aux pratiques en premier lieu, avant d’étudier la manière dont celles-ci se déroulent dans un cadre technologique bien précis.

4.1 Via les pratiques

4.1.1 Identité digitale

Le premier moyen d’instaurer une relation de confiance, nous l’avons vu plus haut, est d’établir cette relation avec une personne, ou en tout cas une identité persistante si la relation en face à face est impossible. Une fois que cette relation se déploie dans le temps, « des informations plus ou moins crédibles sur le fait qu’un individu est digne de confiance s’accumulent » (NOOTEBOOM, 2006, p. 71). Lorsque cette accumulation d’informations est suffisante, la confiance peut s’instaurer.

Cette accumulation d'informations doit avoir lieu sur un même pseudonyme, afin de ne pas être diluée entre plusieurs identités. D'où l'importance de se créer une identité numérique persistante sur les DNMs, et de la conserver le plus longtemps possible

```

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

/u/AnEvilKangaroo is the reddit account controlled
by /u/wombat2combat since the old account got suspended.
-----BEGIN PGP SIGNATURE-----

iQJ8BAEBCgBmBQJasrnrXxSAAAAAAC4AKG1zc3VlcilmcHJAbm90YXRpb25zLm9w
ZW5wZ3AuZmlmdGhob3JzZW1hbi5uZXQ2QkNCM0I1NjNENzZGRkQ3QzQ4MDgyOTIz
MOM2ODc5NDUwMkQzNjZGAaoJEDPGh5RQLTzvegYP/1fw8pknQfhFfhWF/xUroXYE
+6LFRv8G0x2LWJ7TFis9VeznWwvT+KuVGt67z/CQg22p3mTQsGgkZtHDMWxbb4c1
epvHd/d27/+cqQepH+X6kBUv8Qaq/Jd3q0vcP2QLI6btNgndwq2G1E2pAK8CbiO
iyjfwPvZ95jt4UGZvi4kAo3Ofmq1jdJY6/SFGGLmPAHj5WLi19nupu2hMuGSfGPu
lXQOr8v3QaC4FoDzK0TfZzR+s6UCff4vvQGfPuHxycLCUyQ1YONuWknhGF3YFe2K
gx6Xhm5DYr8A4xOijz4K0+nFWWUIjppOw7ect8HLM7m5IcZb1aLT/d63+vuWt0Ta
U1tgghEkHp8oVBP9hubgH1qeGudG4hQKustZMnWVgQ/teauP6z73pMEUBL6bdxzQ
AE+QK+LFZd8fYnHwn3kt18GO9Ln4Pr4Ty+cVoX8EViTzhV/VoLTjR+Vhx99cDg99
a2Yqg0dwbZ5m6e/B4poDD6CGhKdVJIHxrOFCl2G2KwJIJKAsRahYMEpq/h/UIF7
DNw5i3nE6GdBNuvdYvYr71D3QnVTI/ASDmOY7EQu72w3Dd6v1/f0ErvE1Eh0E5fM

```

FIGURE 4.1 – Un modérateur de /r/DarknetMarkets change de compte après avoir été banni

La figure 4.1 est une capture d'écran réalisée sur Reddit quelques heures après que le site ait banni la majorité des subreddits en lien avec les DNMs. L'utilisateur *wombat2combat* était un modérateur de /r/DarknetMarkets, et fut pris dans la vague de bannissements.

Personnalité à la réputation importante, puisque modérateur depuis très longtemps, il put transférer son identité numérique vers un compte nouvellement créé, *AnEvilKangaroo*. Ce transfert n'aurait pas été possible en créant simplement un nouveau compte qui aurait posté « Je suis le compte contrôlé par *wombat2combat* », et l'utilisation de la technologie PGP, dont le fonctionnement sera détaillé plus bas, permet de confirmer l'origine du message. L'accumulation d'informations liées à *wombat2combat* fut ainsi transférée à *AnEvilKangaroo*.

La première étape pour chaque acteur dans les DNMs est donc de se créer une identité numérique persistante, afin de pouvoir y associer petit à petit des informations par rapport à sa fiabilité, et se construire une réputation positive.

Si c'est là la seule possibilité pour les acheteurs de se construire une identité, les vendeurs ont un autre moyen à leur disposition : la création d'une marque. Sur Internet en effet, « les consommateurs devant faire un choix parmi plusieurs options de qualités incertaines se reposent sur la marque, le prix, et la réputation du vendeur comme autant de gages de qualité »¹(AMBLEE et BUI, 2008, p. 2). Les prix étant à peu près constants au sein d'une même plateforme pour la plupart des produits, des marques

1. Ma traduction. Citation originale : « Consumers choosing among competing brands about whose quality they are uncertain rely on brand name, pricing, and retailer reputation as signs of product quality. »

se développent alors afin de se distinguer du reste. Sur le marché de la MDMA, deux fabricants tirent leur épingle du jeu : Checkpoint (CP) en Europe, et G6 en Amérique du Nord.

100x CP Pink Supreme MDMA Pills ~220-250MG

Vendor	RollingBones (1) (5.00★)
Price	฿0.173 (\$1291.68)
Ships to	United States
Ships from	United States
Escrow	Yes



FIGURE 4.2 – Un revendeur de pilules de MDMA produites par CP

Chaque fabricant sort à intervalle régulier de nouveaux designs. En matière de LSD il peut s'agir de buvards formant un motif particulier lorsque mis côte à côte, et en matière de MDMA la différence se joue au niveau des logos présents sur les pilules : Pink Supreme comme montré figure 4.2, Oreo, Pikachu, Tesla, et ainsi de suite. Les utilisateurs font leur choix en fonction du fabricant, comme le montre ce message de *blatantpanda* sur */r/MDMA* :

« CP > G6 from experience with consumptions and friend feedback. I've felt with every CP and G6 press and usually the first to know about upcoming G6 presses. I prefer the higher dosage, and majority of old G6 presses gave me a bad headache or too speedy feel mainly with the pikachus. The recent G6 presses are way better quality and consistent, but will always choose a CP over them any day. »²

Ces diverses stratégies permettent donc de créer des identités numériques avec lesquelles les acteurs peuvent interagir. Néanmoins, réaliser ce saut dans l'incertitude comporte toujours des risques si la relation vient de débiter. Le travail de Pilisuk et Skolnick détaille un moyen de créer la confiance dans le cadre d'une relation où les risques sont élevés pour les différents acteurs impliqués : « A set of small, unilateral, conciliatory overtures each preceded by an announcement and carried out without guarantee of reciprocal overtures. After several such moves, non really sacrificing

2. Message accessible ici : <https://goo.gl/B4o2r8>, accédé le 26.07.2018

security, reciprocation leading to a reversal of the arms-suspicion deadlock could be anticipated » (PILISUK et SKOLNICK, 1968, p. 121).

Sur les DNMs, cela consiste à l'achat en premier lieu de petites quantités de produits, afin de s'assurer de la fiabilité d'un vendeur. L'avantage pour le vendeur est le même : s'il s'avère que l'acheteur ne compte pas payer, celui-ci ne risque pas une perte trop importante. C'est la stratégie employée par *organichewn*, dont l'entretien est visible annexe A :

« En général je commence par acheter un échantillon, pour vérifier la stealth³ du vendeur et voir si effectivement je reçois quelque chose. Si tout joue je passe à une vraie commande. »

Dans le cadre étudié ici, nous avons donc affaire à une confiance fondée sur la connaissance, c'est à dire sur l'empathie. Cela permet aux partenaires d'élaborer des cadres cognitifs commun, et de construire une relation stable dans le temps (NOOTEBOOM, 2006, p. 71).

4.1.2 Évaluations & réputation

« You can check the source code of the addon and see that it is not malicious. I would not ruin my whole account and reputation just to maybe get one or two buyers with a malicious addon. »

Ce message fut posté sur /r/DarknetMarkets par un modérateur, après qu'il ait publié un programme open source permettant à la communauté d'améliorer et de faciliter l'utilisation des DNMs. De nombreux utilisateurs s'étaient montrés réticents à l'installer, de peur que l'addon ne contienne du code malicieux. La justification du modérateur montre à quel point, sur les DNMs, la réputation est l'élément charnière autour duquel s'articulent les interactions.⁴ Selon Alpcan, « un individu décide de faire confiance ou non à une identité numérique en se basant sur la réputation de cette identité » (ALPCAN et al., 2010, p. 1). Plusieurs facteurs influencent notre avis sur un agent donné : la pression de groupe, la timidité, les connaissances de base, etc. Un équilibre est atteint une fois que les avis des membres ne changent plus et restent constants.

L'un des problèmes majeurs en matière de commerce sur Internet, et de manière plus générale en matière d'interactions sociales à distance, réside dans l'asymétrie de l'information. L'une des deux parties aura toujours un meilleur accès que l'autre à l'information, qu'il s'agisse de la qualité d'un produit, de la fiabilité d'un fournisseur ou de la rapidité de la livraison par exemple. Ce problème précède largement les

3. *Stealth* est un terme difficilement traduisible en français, et correspond à la manière dont un colis envoyé par un vendeur est construit pour échapper à un contrôle aux douanes.

4. Le message sous-entend également que, si cela ne vaut pas la peine de ruiner sa réputation « just to get one or two buyers », le jeu pourrait en valoir la chandelle dans d'autres circonstances.

DNMs, et sa solution a toujours été l’instauration de systèmes de réputation plus ou moins formalisés.

Au Moyen-Âge par exemple, de nombreux marchands européens pratiquaient le commerce au Maghreb. Etant donné la lenteur des communications à l’époque, ils envoyaient des émissaires gérer les affaires en leur nom. Ne pouvant pas vérifier si leurs agents respectaient les consignes et ne profitaient pas de la distance pour détourner de l’argent à leur profit, les “Maghribi traders” mirent en place un système de réputation. Au sein de ce système, les commerçants, alors réunis en une coalition, récompensaient les agents les plus efficaces en leur donnant le plus de travail. Si un agent s’avérait ne pas être digne de confiance, toute la coalition refusait de faire affaire avec lui (GREIF, 1989).

Au sein d’un tel système, il est dans l’intérêt de chacun de mener à bien sa tâche : les agents s’assurent ainsi d’être récompensés par un travail -et donc un revenu- constant, et les commerçants sont sûrs d’avoir affaire à des agents honnêtes. Ce système de réputation informel est aujourd’hui formalisé sur Internet, où chaque transaction peut donner lieu à une évaluation, et donc à la construction d’une réputation pour le vendeur.

Sur les marchés du darknet, une fois l’identité d’un vendeur établie, l’accumulation d’informations à son propos vise à établir et maintenir une réputation positive, qui peut être ensuite mise en jeu pour proposer différents services. La figure 4.3 montre comment la réputation d’un vendeur est présentée sur Dream Market

Vendor [Qualitywhitee \(3450\) \(4.78★\)](#) (👤 1000, 4.888/5)
 (₿ 95/1/4) (📧 5877/111/143) (✈ 100~200, 5.00/5) (M #141, 9.52/10) 🛡
Price ₿0.001736 (€10.4)
Ships to Worldwide
Ships from germany
Escrow Yes

FIGURE 4.3 – La réputation du vendeur *Qualitywhitee* sur Dream Market

Cette réputation comporte plusieurs informations :

- Le nombre de transactions réalisées (ici, 3450)
- La moyenne des évaluations reçues (ici, 4.78 sur un maximum de 5)
- Ces mêmes informations pour d’anciens DNMs : Agora, Black Bank, AlphaBay, Abraxas, et Middle Earth Marketplace

Cette accumulation d'informations permet de déterminer si un vendeur peut être déclaré comme digne de confiance ou non.⁵ Sur Dream, cette appellation donne le droit à un vendeur de demander le paiement direct à ses clients, sans que le marché ne fasse office d'intermédiaire.⁶ Les figures 4.4 et 4.5 montrent le cas d'un *trusted vendor*, ayant reçu une moyenne de 4.96/5 après 2300 évaluations, et celui d'un vendeur ne disposant pas de l'appellation et n'ayant donc pas le droit de demander à ses clients de FE.

Username Nestea93 (2300) (4.96★)
Trusted seller Yes ✓
FE enabled Yes
Join date 17/09/2017

FIGURE 4.4 – Un *trusted vendor* sur Dream Market

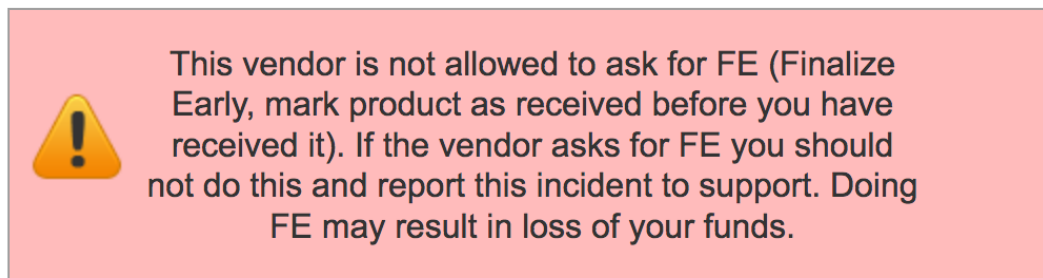


FIGURE 4.5 – Un vendeur qui n'a pas la réputation suffisante n'a pas le droit de demander à ses clients de "FE"


L'intérêt de la construction d'une réputation positive est donc en premier lieu d'être payé plus rapidement qu'un vendeur ayant une réputation médiane. Le deuxième avantage est que la réputation fonctionne de la même sorte qu'une « assurance risque » (BOTSMAN, 2017). Les vendeurs de bonne réputation étant considérés comme posant moins de risque que les autres, ils peuvent alors exiger de leurs clients un prix plus élevé. Pour le cannabis, cette "assurance" peut valoir \$0.45/gramme, soit près de 5% du prix au gramme (ibid., p. 145).


La réputation est également utilisée en cas de conflit entre deux parties, comme montré figure 4.6.

Il arrive en effet que, suite à une transaction, l'acheteur déclare ne pas être satisfait. Cela peut être dû à la mauvaise qualité du produit, au poids insuffisant, voire tout simplement au fait qu'il n'a rien reçu. Se lance alors une procédure de contestation, *dispute* en anglais. Acheteur et vendeur sont mis en relation avec un modérateur envoyé par le marché, et doivent chacun donner leur point de vue à propos de la transaction en

5. C'est ce qui ressort des expériences des utilisateurs *_da_da_da*, *pouetpouet123456* et *organichewn*, visibles annexe A. Ces trois utilisateurs des DNMs se basent, entre autres, sur le nombre d'évaluations reçues par un vendeur avant de faire leur choix.

6. Il s'agit de la pratique dite du *Finalize Early*, ou FE, dont nous parlerons plus tard

	Sent by Botah Moderator on Mar 19, 2017
Botah Moderator	Buyer pls explain the issue with your order, and vendor feel free to defend yourself. There is a dispute FAQ on my profile for buyers to read.
Joined: Feb 16, 2016 Msgs: 20666 Trust: Level 5	Buyers can speed up the dispute process by checking vendors profiles to see the last time the vendor signed on. If they have not signed on in 4+ days, we can issue you a refund.
	If you would like to finalize the sale, please do so by going to the order page and releasing the full amount in escrow, vendors can do the same to refund a sale. You do not need to wait for a moderator. Please only send 1 message every 24 hours so we are able to keep our volume of messages lower.

	Sent by HubertBonisseur New Member on Mar 19, 2017 at 18:46
HubertBonisseur New Member	I ordered 5g of MDMA 17 days ago (the 2nd of March) and it still hasn't arrived. I didn't get a love letter either (yet), so maybe the package got lost or something.
Joined: Nov 11, 2015 Msgs: 10 Trust: Level 5	


	Sent by SimplyWild1 Vendor on Mar 20, 2017 at 01:04
SimplyWild1 Vendor	Im sorry that the package is not arrived in the discribed amount of days. Im sure from our side there was no problem shipping your order. At this time i can offer an 100% reship or an 50 % money refund.
Joined: Jul 28, 2016 Msgs: 8915 Trust: Level 5	With best regards, SW

FIGURE 4.6 – L'interface de *dispute* sur AlphaBay.

question. Si un consensus est atteint la contestation est considérée comme résolue, mais si cela n'est pas le cas c'est au modérateur de prendre une décision et de déterminer qui doit recevoir les fonds. L'interface montrée 4.6 nous permet d'imaginer quels sont les éléments permettant au modérateur de trancher : la date d'inscription de chacune des parties, son nombre de messages envoyés, et son niveau de confiance, ce dernier étant déterminé par la plateforme de manière automatique.

Un effet secondaire de ces systèmes de réputation concerne le transfert des savoirs

en matière de drogues. Avant que les DNMs ne se développent, seuls les vendeurs possédaient la connaissance par rapport à la pureté, la fabrication, ou encore la puissance du produit vendu. Ces savoirs sont, avec les DNMs, disséminés au sein de la communauté des acheteurs, dont certains agissent alors comme des « nœuds centraux de savoir » (BANCROFT et REID, 2016, p. 14).⁷ De plus, n'importe quel acheteur étant invité à laisser son avis, une certaine objectivité est alors possible : « l'avis rédigé du consommateur profane doit lui permettre de laisser libre cours à sa subjectivité ; c'est en effet l'accumulation et la multiplication des récits subjectifs, parmi lesquels l'internaute est libre de naviguer, qui garantit la formation d'un jugement objectif. » (BEAUVISAGE, BEUSCART, MELLET et al., 2014, p. 180).

4.1.3 Documents d'identité et tiers de confiance

Au sein d'un groupe de criminels, deux moyens existent d'instaurer des relations de confiance (STRUB et PRIEST, 1976) :

Schéma de dévoilement Ce schéma consiste à montrer, petit à petit, des “documents d'identité” vérifiant la légitimité d'appartenance au groupe. Ce schéma est d'autant plus important dans un cas tels que les DNMs, où ces documents sont la seule base sur laquelle il est possible de former un avis. Cela signifie qu'un nouvel arrivant sur un forum de discussion lié à ces marchés sera contraint de montrer patte blanche s'il veut pouvoir s'intégrer, en parlant par exemple de ses expériences passées avec telle ou telle substance ou en utilisant le langage vernaculaire propre à la communauté au sein de laquelle il participe. Mais, comme précisé au cours du chapitre 2, se montrer trop entreprenant pour s'intégrer peut créer le soupçon.



FIGURE 4.7 – Nice try officer

Comme la figure 4.7 le montre, un nouvel arrivant posant trop de questions à la fois se verra répondre « Nice try officer », signe que son jeu ne passe pas inaperçu et qu'il a été démasqué. Peu importe qu'il s'agisse ou non d'un officier de police, il s'agit là d'une des nombreuses conséquences de l'*Operation Bayonet*. Pour pouvoir s'intégrer

7. Key knowledge nodes

dans l'écosystème des DNMs, il est nécessaire d'avoir un compte qui ne soit pas trop récent,⁸ et de s'en être servi pour interagir avec les autres utilisateurs.

Schéma d'extension La philosophie de ce schéma est celle du tiers de confiance : si un agent fait confiance à une entité A qui fait elle-même confiance à une entité B, alors l'agent initial fera lui aussi confiance à l'entité B.

Cette idée est derrière le système d'*escrow* en vigueur sur les DNMs. Celui-ci consiste pour un acheteur à laisser l'argent nécessaire à une commande sur un portefeuille contrôlé par le marché. Une fois la commande marquée comme reçue, le marché débloque alors les fonds et transfère l'argent sur le compte du vendeur. Cette idée part néanmoins du principe qu'un marché est plus digne de confiance qu'un vendeur, ce que les différents *exit scams* réalisés tout au long de l'histoire des DNMs tendent à infirmer. Néanmoins, c'est selon ce principe que les DNMs opérant aujourd'hui fonctionnent.

Le problème pour les vendeurs est double : ceux-ci ne sont pas payés immédiatement après la transaction, mais parfois plusieurs semaines après si un client oublie de finaliser la commande, et ce qu'ils reçoivent peut ne pas correspondre au prix initial. Le bitcoin étant en effet sujet à de fortes variations, il peut tout à fait perdre 25% de sa valeur en quelques jours. En revanche, si le cours de la monnaie vient à subir une forte hausse, cela est là aussi au désavantage des vendeurs. Un client peut scrupuleux peut en effet décider de contester la commande, et espérer que le marché tranche en sa faveur. S'il récupère la totalité de ses bitcoins, il aura non seulement reçu sa commande initiale gratuitement, mais pourra commander une plus grande quantité de produits avec la même quantité de bitcoins.

Pour cette raison, de nombreux vendeurs demandent à leurs clients de FE, c'est à dire de déclarer la commande reçue aussitôt celle-ci passée sur le marché. Cette pratique comporte néanmoins des risques, comme le dit *organichewn* : à chaque fois que celui-ci a perdu de l'argent, c'était dans le cadre d'une transaction où il avait FE. Dream Market met également en garde ses utilisateurs contre cette pratique, nous l'avons vu figure 4.5.

Au delà des marchés, d'autres tiers de confiance existent : les modérateurs des forums disposent d'un certain pouvoir de persuasion, de même que les utilisateurs réalisant de nombreuses critiques à propos des vendeurs qu'ils utilisent.

Le cas de Energy Control⁹ (EC) est particulièrement intéressant. Il s'agit d'une ONG espagnole disposant de matériel permettant la réalisation d'analyses chimiques poussées, et qui propose comme service d'analyser les substances reçues par la poste. Les résultats sont ensuite renvoyés sous forme de fichier PDF à la personne ayant envoyé la substance. Ces résultats peuvent ensuite être utilisés par les clients lorsqu'ils

8. Avant sa disparition, /r/DarknetMarkets apposait notamment l'étiquette *Fresh Account* à côté des pseudonymes d'utilisateurs ayant été créés moins de 24h avant leur arrivée sur la plateforme.

9. <https://goo.gl/qeVxj2>, accédé le 28.07.2018



FIGURE 4.8 – Un vendeur sur Aero signale que sa cocaïne a été testée en laboratoire par Energy Control

publient leurs critiques sur Internet, mais également par les vendeurs : sur la figure 4.8, le vendeur *FastFoodUK* précise que sa cocaïne est, d'après Energy Control, pure à 92%. L'ONG mentionne toutefois cette pratique dans sa FAQ :¹⁰

Our drug testing service is specifically designed for final users. The results we offer are only valid if the sample used is exactly the same as the sample tested previously. None of our results can be used as a quality guarantee from any drug vendor or product. Energy Control declines all responsibility in this sense.

Le service proposé par EC étant payant, certaines communautés se proposent de mutualiser les dépenses et de partager les résultats obtenus en laboratoire. C'est notamment le cas de DNMAvengers,¹¹ qui met chaque mois à disposition de ses membres une cagnotte dont ceux-ci peuvent se servir pour faire analyser leurs substances. Il s'agirait alors ici d'un schéma de double extension, puisqu'un utilisateur de DNMAvengers doit faire confiance non seulement à Energy Control, mais également aux utilisateurs pour qu'ils postent les résultats réels renvoyés par l'ONG.

4.2 Via les technologies

4.2.1 Moyens d'accéder au réseau (TOR)

Nous avons vu au début de ce travail qu'un darknet market est une place de marché du deep web, accessible via le darknet. Ces DNMs ont des URL se terminant en *.onion*, et non *.com* ou *.ch* comme on peut en avoir l'habitude, et nécessitent l'utilisation d'un navigateur bien précis pour y accéder : Tor, qui signifie *The Onion Router*.¹² Lorsque un utilisateur lance ce navigateur, comme nous pouvons le voir figure 4.9, plusieurs

10. <https://goo.gl/nP72J8>, accédé le 28.07.2018

11. <http://avengersdutyk3xf.onion>

12. D'autres moyens existent pour accéder au darknet : i2p, qui est un système semblable à Tor, ou même des extensions pour les navigateurs classiques. Ces cas de figure dépassent le cadre de ce mémoire, et ne seront pas étudiés ici.

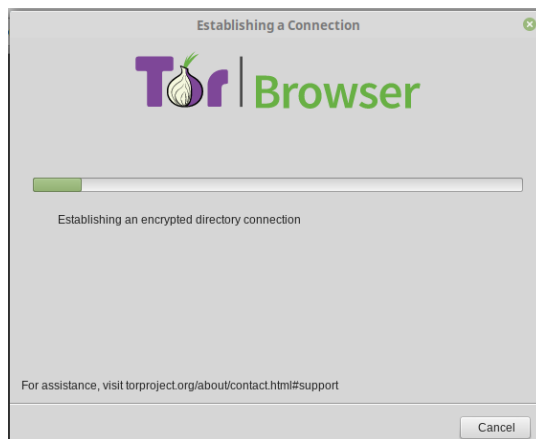


FIGURE 4.9 – L’interface de connexion à Tor

nœuds sont trouvés pour établir une connexion. Ces derniers sont des machines mises à disposition du réseau par des membres volontaires, et permettent la mise en place d’une connexion sécurisée aux sites visités.

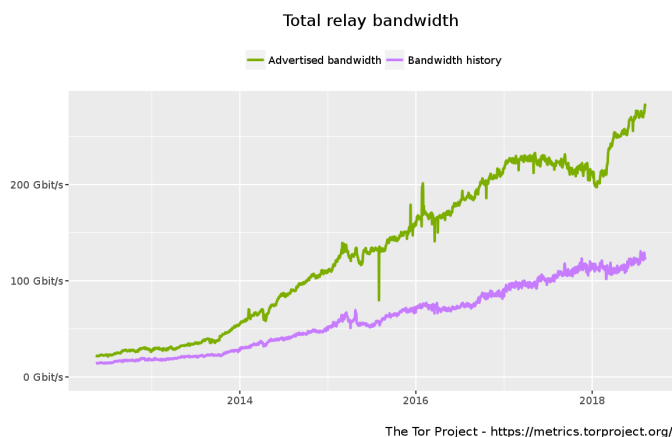


FIGURE 4.10 – Evolution de la bande passante de Tor

Lorsque la machine client envoie un paquet à un serveur, ce paquet doit passer par n nœuds, chacun disposant d’une clef de chiffrement. Le paquet est chiffré n fois avant de partir du client, par les n clefs de chiffrement. Quand il arrive au nœud 1, il est déchiffré par la clef correspondante et envoyé au nœud 2, qui le déchiffre à son tour. Ce processus continue de la sorte jusqu’au n -ième nœud, qui envoie finalement le paquet en clair à sa destination finale. Ainsi, aucun nœud hormis le dernier ne peut connaître le contenu du paquet, mais le dernier nœud ne pouvant pas savoir qui a envoyé le paquet cela n’a aucune importance. Le premier nœud connaît l’adresse IP de l’utilisateur, mais pas sa destination finale ou son contenu.

La connexion est donc sécurisée de bout en bout par ce système, et n’est à priori pas vulnérable à des techniques poussées telles que le *deep packet inspection*.¹³ De plus,

13. Néanmoins, un gouvernement pratiquant le DPI peut tout à fait réaliser qu’un paquet est destiné à Tor et bloquer la connexion, même sans en connaître le contenu précis. Pour plus d’informations, voir : <https://goo.gl/YJWr4>, accédé le 28.07.2018

même si le fournisseur d'accès d'un utilisateur de Tor peut voir que le client est sur le réseau, il est impossible pour lui de savoir quels sites sont consultés ; et l'utilisation d'un VPN permet même de camoufler entièrement la connexion à Tor. Le désavantage d'un tel système réside dans sa vitesse : celle-ci sera en effet celle du nœud le plus lent, et dépendra également du nombre de nœuds disponibles par rapport au nombre d'utilisateurs. La bande passante du réseau ne cesse néanmoins d'augmenter depuis son lancement, comme le montre la figure 4.10.

4.2.2 Systèmes d'exploitation

L'accès aux DNMs laisse néanmoins des traces : adresse physique de l'ordinateur connecté au réseau, fichiers temporaires présents sur la machine, opérations réalisées par le processeur, etc. Toutes ces traces peuvent agir comme autant d'indices pouvant donner lieu à l'arrestation d'un utilisateur, comme ce fut le cas pour Ross Ulbricht. Plusieurs systèmes d'exploitation (OS) visant à minimiser ces traces existent.

TAILS **The Amnesic Incognito Live System**¹⁴ est un OS destiné à n'être utilisé que depuis une clef USB, d'où sa qualification de *live system*. Une fois installé, l'utilisateur a le choix de créer un volume de données persistant chiffré sur la clef USB, restauré à chaque nouveau lancement si le mot de passe correspondant est saisi. En dehors de ce volume persistant, le système est réinitialisé à chaque utilisation et ne propose que certaines applications de base : Tor, un client mail, et un logiciel PGP. Des options de sécurité poussées sont proposées au démarrage, et permettent par exemple à l'utilisateur de modifier l'adresse physique de sa machine lors de la connexion au routeur.

Qubes Cet OS¹⁵ a pour but de régler le problème de "monolithicité" de Tor, signifiant par là que, sur Tor, toutes les applications tournent sous le même OS. Si la session est compromise, toute l'activité de l'utilisateur peut l'être. Qubes fonctionne selon le principe de compartimentation, en proposant à l'utilisateur d'utiliser des *qubes* isolés les uns des autres. Ces *qubes* fonctionnent sur le même principe que des machines virtuelles, mais dépendent directement du matériel de l'ordinateur et ne dépendent pas d'un programme (au contraire de VMware ou VirtualBox). Un utilisateur peut donc avoir son activité liée aux DNMs isolée au sein d'un *qube*, et utiliser un autre *qube* pour toutes ses autres activités légales.

Whonix Contrairement à Qubes et Tails, Whonix¹⁶ n'est pas un OS à part entière, mais un *desktop OS*. Celui-ci propose d'interagir avec une version fortement modifiée

14. Disponible ici : <https://goo.gl/xGoXo6>

15. Disponible ici : <https://goo.gl/jxDyDa>

16. Disponible ici : <https://goo.gl/zauXQ4>

de Debian,¹⁷ tournant au sein de plusieurs machines virtuelles imbriquées les unes dans les autres. Les activités réalisées sur Whonix sont ainsi isolées du reste de la machine, et même des virus disposant d'un accès *root* n'auront pas accès aux informations sensibles comme l'adresse IP. Comme sur TAILS, certaines applications de base sont installées par défaut.

Ces trois exemples ne sont pas exhaustifs, mais permettent de donner une bonne vue d'ensemble des possibilités offertes aux personnes souhaitant protéger leur vie privée au maximum. Ils peuvent être utilisés ensemble, en faisant par exemple tourner Whonix au sein de Qubes ou TAILS, ou en rajoutant une surcouche VPN par dessus.

4.2.3 Communications chiffrées et identités persistantes

Nous avons vu au cours de ce travail à quel point il était important de pouvoir disposer d'une identité persistante sur les DNMs, n'étant pas forcément liée à un pseudonyme ou une plateforme particulière. Le système utilisé pour cela porte le nom de PGP, pour *Pretty Good Privacy*,¹⁸ et fonctionne via l'utilisation de clefs de chiffrement privées et publiques. Chaque utilisateur dispose d'une paire de clefs, la privée restant confidentielle et la publique étant mise à disposition des personnes souhaitant communiquer avec lui. La figure 4.11 montre la manière dont une clef PGP publique peut être présentée. Ce système permet la mise en place de deux pratiques primordiales sur le darknet.

Public PGP key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFm+no8BEADlxush9akHIi7VsDZmEjN0eywFm5PGXaYE6m79pG+UJn0oIAuo
pHgTDvsnT276KG7FsaDIbEUlgsV4SvP5C71aZ/6E+XYSwvcuoFwuv0rotQmDghpU
2gFN7zs5pCgAo+kLNFb0gbH/eica/Kx1heXlXmEA1+juKiFfjn3heK5h39XPG1J2
SUGns0U13hmBg021LJMN5c5jusRvFt6JY0x/zB2nW3eeYwWLeb2LPXj0Cgkjp1nM
f0FMyclHfdZP0art1npBcIYxTV3s01ymEZ5na5cga4yHaBnZ7R+W08SAVSnwIQQj
yn5/+1+4gfUupo4i1cJhIS6RRQj4XqVuvEQ8YTHaQoxA1e57PkgeQGeS73cn3evM
tE36Y4y9C+j+zIXmRXwhsTtOE3Xum3Z1m/XHW5NITsxBDLreN7mi/m4cRZ9Tn47C
QBC4EUmbuRwGcstoc0QsGcBLdI9o+TNPgqvUoHD+9XIiSoXVZBvpKF88yV0M7h
zfhgFJx1JtdMebytbMyRWCCeom7wcNnJO+8biq3t1vtC61cTFbj7R5vs1+dBw/Zf
+1DBdC20K70bnKrdVkdT6Q1YpIrixkZyq8Lzb0GRd8QvAYm+jYghbA6loaos3fW
T8hEwHwXsZcr2PnmZMCGwqXwQz/OzdNwSH2VrLFxHzdGSZCYeVhSCT9JwARAQAB
tCx0ZXN0ZWE5MyAobGvtb24gb3IgcGVhY2gpdX0Z0Z0ZWE5M0BmdHAUz292PoKc
PAQTAQoAJgUCWb6ejwIbAwUJCWZTUQLCQgHAWUVCgkICwQWAgEAAh4BAheAAAoJ
EPc1f2jTXLPL3tYP/1NChcJsokC6W5ng5MZFMT31C6pPaF8DYDoct/GBHwXdtY
ZbAQx26N6NQLCksmiLc+cbr3iPwL61YeBPJo8m77B92n8MF0J/8Sc/asvAX/ZvEn
4zZKYLZCXeqa0d+ZZTI/OzCucoFM16btv69YIsik/CaVF9i/rULX9vwbMdxj1f4j
OUXi0jkdhvJUYSzpnPH25FkCaQ0kyr7rudGdbv6fTsREGK+EMkzcm+2fwY20E8B
yj3UGzBvdZRF5M9ihhf5ZotJ3N0fr92v7/c1Bo4q0gJ2hewU1a8T3XRJKR2Ss+J
afbhd7Dh5qt8KY7bLQ0fPDVd2aE1ru86AYX0nyBXQ4UFiXsu5TZZU/Anfwm+vDsa
3f3doySvaur4/lXayeKU82nxav32idnaB9IP27N5ayl0QCfRkND7mRB+2QEgh07J
8MIPCFcxwAqTBiclvJcyKkZ1ugzgggepPASNiDbQDCfe03+AeJC5Fpmw/IbUVM0+6
0kiH1gq1vQN2Jo0eZ186kdsyZ5SsPtBxxmpBjU2kt8rSpx9HBipfnk+vL2JISiC
```

FIGURE 4.11 – Le début de la clef PGP publique d'un vendeur sur Dream

17. Debian est un OS open source dont le développement a débuté en 1993.

18. Assez bonne confidentialité.

Authentification Un utilisateur, Alice, souhaitant authentifier son message peut l'envoyer précédé d'un condensat, chiffré à l'aide de sa clef privée. Si Bob, un autre utilisateur, souhaite vérifier que le message provient bien d'Alice et qu'il est authentique, il déchiffre le condensat à l'aide de la clef publique d'Alice, puis calcule lui même le condensat du message. Si les deux condensats concordent, cela signifie que l'expéditeur du message est bien Alice, et que le message n'a pas été altéré depuis sa rédaction. C'est cette fonction d'authentification qui est mobilisée dans l'exemple de la figure 4.1, où *wombat2combat* transfère son identité numérique sur un nouveau compte.

Confidentialité Si cette fois Alice souhaite envoyer un message à Bob sans que celui-ci ne puisse être lu par une tierce personne, elle peut le chiffrer en utilisant la clef publique de Bob. Lorsque Bob recevra le message, il pourra le déchiffrer en utilisant sa clef privée. Seule la clef privée de Bob peut être utilisée pour déchiffrer le message, et cela garantit la confidentialité de la communication. De plus, en chiffrant le message, Alice peut signer le chiffrement à l'aide de sa clef et montrer à Bob qu'elle est bien la personne à l'origine du message. Cette pratique est au cœur du fonctionnement des DNMs, et permet à un client de transmettre son adresse et son nom à un vendeur sans que ces informations ne puissent être lues par autrui.

Certains DNMs proposent de chiffrer directement dans le navigateur les communications entre acheteurs et vendeurs : en stockant la clef publique d'un vendeur sur leur serveur, il peuvent en effet recevoir le message en clair, le chiffrer, et le transmettre à son destinataire. Cette pratique comporte néanmoins un risque, puisque le marché a, à un moment donné, accès au message en clair, qui peut alors être intercepté, voire stocké. Il est alors recommandé de ne jamais utiliser cette fonction, et de prendre le temps supplémentaire de chiffrer le message depuis une machine considérée comme sécurisée.

4.2.4 Cryptomonnaies

La chute de TFM, discutée au début du chapitre 3, fut en partie due à l'utilisation de moyens de paiements "classiques", permettant d'envoyer de l'argent à des identités civiles : PayPal et Western Union. Pour cette raison, les DNMs aujourd'hui utilisent des cryptomonnaies. Le BTC principalement, dont le fonctionnement a été détaillé plus haut, mais également l'Ethereum (ETH) ou Monero (XMR).

Ces monnaies nécessitent simplement la création d'un portefeuille virtuel pour être utilisées, et peuvent être stockées sur un disque dur non connecté à internet. Pour procéder à un échange, seule l'adresse du portefeuille du receveur doit être connue.

Dans le cas du Bitcoin, chaque transaction est publiquement enregistrée sur la blockchain, et plusieurs informations sont publiquement accessibles : adresses de l'envoyeur

4aa2322e7359069e5ba3d8acee64ec773a3ee080212cf7d551c98400515ab2	2018-08-13 14:33:23			
1MjwPHZQWewf8G82pVkwQWEJ9LjgSA1bDS	→	1JCCk5VG3gD74bV3eNvELQCwFjNv4TxWc 15L8UK2BACkeZygsJY7eYyYqJqHwvepR	0.0005 BTC 0.00101146 BTC	0.00151146 BTC
5c1b417b9ebae798ba34a713f2da6c32fba12043d2920bb61721b36301e	2018-08-13 14:33:21			
19nhou4y1LKJv4oWJ25KVLMTuLmjabuqn	→	1BVFmQxcvEfy2DKZyzPT6E4yKUAec 1BAFmFwyEV9SjMTaY4Wwyan5c4PFVnh2z8	0.0105 BTC 0.80560977 BTC	0.81610977 BTC
6ac0dad7ea84b19959e6573c37f9858ee300697572058bd5203d514f69a750a	2018-08-13 14:33:18			
1LhrfB5NhY7d8smvYGYMqnDV62RMnAbGZq	→	199ZAvZeKo8L1whYyjsUCVs2mPq3Dpmm 12yq9s7y7svXjMEEGobYPTYb26ZKEi9zpf	0.003091 BTC 0.22551925 BTC	0.22861025 BTC

FIGURE 4.12 – Un extrait de la blockchain du Bitcoin

et du receveur, date et heure de la transaction, et montant de la transaction notamment. La figure 4.12 est un extrait de la blockchain du Bitcoin, tiré du site <https://www.blockchain.com/explorer>. Le fait que tant d'informations soient publiques pose problème lorsque l'on s'intéresse aux DNMs, puisque cela met à mal l'anonymat présent partout ailleurs sur le réseau. Les BTC doivent en effet s'acheter avec de l'argent classique, sur des plateformes en ligne ou bien entre individus. Ces achats laissent des traces, qui peuvent être remontées pour connaître toutes les transactions réalisées par l'acheteur, qui peuvent être ensuite reliées à des achats sur le darknet. Si la police sait qu'un utilisateur a acheté une certaine substance pour une somme précise à une date précise, et que Mr. Dupont a réalisé une transaction pour le même montant à la même date, il est compliqué de lui accorder le bénéfice du doute.

Pour résoudre ce problème, des services de blanchiment de bitcoins existent : un utilisateur envoie une certaine somme en bitcoins sur une plateforme, qui lui renvoie la même somme en plusieurs transactions, moins une commission, sur l'adresse de son choix. Même si ces transactions apparaissent sur la blockchain, elles sont toutefois bien plus compliquées à tracer.¹⁹ Le portefeuille *Dark Wallet*²⁰ ainsi que le XMR intègrent ce principe de blanchiment au cœur de leur fonctionnement, et permettent à leurs utilisateurs de ne plus reposer sur des plateformes centralisées pour tenter de rester anonymes.

Multi-sig

Pour qu'une transaction de cryptomonnaie soit réalisée, il suffit en général d'une seule personne, déclarant vouloir transférer la monnaie d'une adresse A vers une adresse B. Sur le darknet, où les fonds sont souvent contrôlés par les DNMs en attendant que le client confirme avoir reçu sa commande, cela est problématique : la porte est ainsi ouverte aux *exit scams* de la part des marchés. L'utilisation de portefeuilles disposant de la technologie multi-sig, pour multi signatures, permet aux utilisateurs de se mettre

19. Mais cela n'est pas impossible. Des entreprises proposent aujourd'hui de désanonymiser la plupart des transactions en bitcoins. Pour plus d'informations, lire <https://goo.gl/Q2ED61>.

20. Accessible ici : <https://goo.gl/g2nuZ2>

d'accord : étant donné que 3 acteurs sont présents dans une transaction sur un DNM (acheteur, vendeur, et marché), trois signataires potentiels existent. Une transaction multi-sig est en général validée à partir du moment où deux signataires sont d'accord. Un marché ne peut alors pas *exit scam* puisque ni acheteur ni vendeur n'auront signé, et dans le cas où l'une des trois parties ne donne plus signe de vie, les deux autres peuvent toujours se mettre d'accord.

4.3 Limites

4.3.1 Sociales

Évaluations Les systèmes d'évaluations entre particuliers se retrouvent aujourd'hui sur un grand nombre de plateformes, mais connaissent plusieurs failles. La première réside dans le fait que, sur les DNMs, ces évaluations sont publiées de manière anonyme. Il est impossible de cliquer sur le pseudonyme de la personne ayant posté un commentaire pour se faire une idée de ses habitudes, ce qui soulève la question de l'origine des commentaires. Un consommateur occasionnel n'aura ainsi probablement pas le même avis qu'un toxicomane qui consomme quotidiennement une substance, mais leurs avis auront pourtant le même poids. Clients et vendeurs ont beau collaborer et devenir par là « producteurs de connaissances et d'expertise » (BANCROFT et REID, 2016), chacun est tout de même invité à prendre en compte son expérience individuelle avant de consommer pour de bon. Tolérance, taille et poids du consommateur deviennent alors des caractéristiques bien plus saillantes que les commentaires qui peuvent être postés sur le profil d'un vendeur.

Il est également possible que des faussaires de la réputation apparaissent, d'autant plus lorsque aucun système de filtrage n'est mis en place. Certains acteurs « exploitent le différentiel de perception entre ceux qui s'en tiennent aux signes et repères communément partagés et ceux qui ont accès à la fabrique de ces repères et de ces signes » (BEAUVISAGE et MELLET, 2016, p. 72), et utilisent ce différentiel pour augmenter artificiellement leurs notes. Il n'est ainsi pas rare de voir qu'un vendeur possède de nombreuses évaluations dithyrambiques, qui ne concernent finalement que des produits valant quelques centimes. On comprend alors que ce vendeur a créé lui-même plusieurs comptes d'acheteurs sur le marché pour s'acheter à lui-même des produits fictifs. Une fois sa réputation établie, des clients véritables peuvent se baser sur ces évaluations fictives pour faire leur choix. Sur les sites « classiques » (TripAdvisor, Yelp, La Fourchette, etc.), des algorithmes permettant de détecter de comportements suspects existent, et des humains sont mis à contribution pour analyser plus précisément les cas difficiles (BEAUVISAGE, BEUSCART, MELLET et al., 2014). Ce n'est pas le cas sur les DNMs, ce qui facilite d'autant plus la tâche de ces faussaires de la réputation.

Hypercentralité de quelques acteurs Le but des faussaires de la réputation est de créer un effet de réseau pour “amorcer la pompe”. Sur Internet en effet, « l’attention déjà reçue par un contenu, sa popularité, constitue le signal le plus puissant pour identifier et sélectionner les contenus les plus intéressants » (BEAUVISAGE et MELLET, 2016, p. 91). La figure 4.3 le montre bien, le nombre de transactions déjà réalisés par un vendeur est un bon indicateur de sa supposée fiabilité. Il s’agit là d’un paradoxe du réseau : pourtant décentralisé, il est fonctionnellement hypercentralisé. Les pratiques se concentrent ainsi de plus en plus au sein de quelques lieux (BEAUDE, 2012), poussant alors les différents acteurs, DNMs comme vendeurs, à tout tenter pour atteindre une centralité maximale. Cela passe par le recours à des fausses évaluations, mais aussi à des attaques comme le DDOS ou le doxxing.²¹

4.3.2 Inhérentes aux technologies utilisées

La plupart des technologies utilisées sur les DNMs sont distribuées, c’est à dire qu’elles reposent sur des nœuds ayant tous le même poids dans le réseau. C’est le cas du BTC, de l’ethereum, mais aussi de Tor. Un réseau distribué part du principe que chaque nœud est “bon”, et qui s’il s’avère que cela n’est pas le cas, le nœud en question peut être exclu du réseau. Le cas de figure où la plupart des nœuds sont corrompus n’est pas pris en compte, mais peut avoir des conséquences désastreuses.

En ce qui concerne le bitcoin par exemple, « if one or more colluding actors were to control at least 51% of the network’s hashing power, they would be able to arbitrarily censor transactions by validating certain blocks at the expense of others. » (DE FILIPPI et LOVELUCK, 2016, p. 11). Cette situation est la plus parlante, puisque si le bitcoin était au départ un réseau décentralisé dirigé par consensus, il est en pratique fortement centralisé et dirigé par une structure de plus en plus oligopolistique (ibid.). Cette crise de la centralité se retrouve également dans les cryptomonnaies disposant de *smart contracts*, où des acteurs contrôlant une grande partie de la monnaie ont un poids souvent critique dans les décisions, et où les tentatives de diminuer ce poids échouent le plus souvent. Si une monnaie décide par exemple d’accorder un nombre de voix dans un vote non pas en fonction du capital mais en fonction de la racine carrée du capital, pour diminuer l’importance des gros acteurs, ceux-ci peuvent tout à fait diviser leur capital entre deux portefeuilles pour échapper à cette mesure. Un paradoxe finit toujours par éclorre : une technologie prônant la décentralisation apparaît, mais se centralise petit à petit pour éliminer les comportements néfastes. Cette centralisation tend à l’apparition d’organismes de contrôles, qui sont précisément ce que la technologie cherchait au début à éviter.

21. Le doxxing, ou doxing est une pratique consistant à rechercher et à révéler sur l’Internet des informations sur l’identité et la vie privée d’un individu dans le dessein de lui nuire. Les informations révélées peuvent être l’identité, l’adresse, le numéro de sécurité sociale, le numéro de compte bancaire, etc. - Wikipédia

Un utilisateur qui se connecte à Tor passe par plusieurs nœuds pour établir une connexion, et nous avons vu comment le réseau était pensé pour que chaque nœud ne puisse pas avoir accès à la totalité de l'information. Or, si tous les nœuds de la chaîne étaient sous le contrôle d'une seule entité, l'utilité de passer par Tor en serait nulle. L'anonymat offert par Tor repose en effet sur l'idée qu'un attaquant potentiel serait incapable de contrôler suffisamment de nœuds pour rendre possible des corrélations, mais ce nombre n'est en réalité pas si élevé. En contrôlant le nœud d'entrée et le nœud de sortie d'une connexion (par exemple en étant en contrôle du site visité, comme ce fut le cas avec Hansa pendant *Operation Bayonet*), un agent pourrait tout à fait procéder à un grand nombre de corrélations en étudiant les paquets transitant par les nœuds, et ce faisant démasquer l'utilisateur.

5 Conclusion

5.1 Familiarité ou confiance ?

Avant d'utiliser une nouvelle technologie ou de faire confiance à un individu, trois questions se posent (BOTSMAN, 2017) :

- Qu'est-ce ?
- Qu'ai-je à y gagner ?
- Qui d'autre s'est déjà lancé ?

Nous avons parlé tout au long de ce mémoire de la manière dont il était possible de faire naître la confiance entre des acteurs, envers des entités, etc. Mais, sur les DNMs plus que partout ailleurs, les réseaux mis en jeu au cours de chaque interaction mobilisent un grand nombre d'acteurs aux identités masquées. Dans de telles conditions, est-il réellement possible de parler de confiance, et ne s'agirait-il pas plutôt de familiarité ?

La familiarité est un sentiment qui repose sur le passé, là où les autres moments n'existent pas (LUHMANN, 2006b). Le passé ayant déjà eu lieu, il est possible de s'appuyer dessus pour décider si une action est risquée ou non. En extrapolant à partir d'expériences passées, les individus peuvent alors imaginer que tout va toujours continuer de la même manière si rien ne vient perturber le système existant (ibid.), et faire comme si le risque était absent de l'équation. C'est en cela que confiance et familiarité sont proches : on fait confiance quand on sait que certains dangers sont présents mais qu'on considère qu'ils ne doivent pas perturber l'action, et un comportement est familier quand on sait que les dangers qu'il comporte ne se sont encore jamais produits. En d'autres termes, la familiarité est une condition strictement nécessaire, mais pas suffisante, à l'apparition de la confiance.

C'est la raison qui fit le succès si fulgurant des *darknet markets* : « people don't want something new, they simply want the familiar done differently » (BOTSMAN, 2017, p. 61). Acheter en ligne est possible depuis des décennies, et les systèmes d'évaluation existent depuis des années. Un nouvel arrivant sur un DNM est donc dans un environnement familier, jusque dans son interface et les pratiques possibles. Seuls diffèrent les produits mis en vente, ce qui diminue le courage nécessaire pour ce premier saut dans l'incertitude, qui n'est alors plus si incertaine que cela.

Et c'est en cela que l'*Operation Bayonet* eut des conséquences si profondes pour les acteurs des DNMs : plus que la confiance, elle vint perturber la familiarité en remettant tout le passé en question. Un vendeur inscrit depuis des années pouvait, d'un coup, être en réalité un agent du gouvernement. La force de cette opération est d'avoir annihilé la confiance des utilisateurs envers les DNMs centraux, sans pour autant leur donner la possibilité de se tourner vers d'autres plateformes : des alternatives aux DNMs centraux existent aujourd'hui, nous en avons parlé au cours du chapitre 3, mais celles-ci reposent sur des concepts envers lesquels le public n'est pas familier : blockchain, marchés décentralisés, Telegram, etc. (HOLLAND, AMADO et MARRIOTT, 2018).

5.2 De l'importance des maillons faibles

Nous avons vu plus haut que les différents moyens sociotechniques mis en œuvre pour créer la confiance sur le darknet n'étaient pas infailibles : chaque étape du processus d'achat peut être détournée pour induire en erreur, les failles discutées en détail n'étant de loin pas exhaustives. Ainsi, plutôt que de se poser la question de savoir s'il est possible ou non de faire confiance sur les DNMs, un utilisateur se questionne plutôt sur le moment où cette confiance sera brisée, et les conséquences potentielles de ce moment. Il ne s'agit alors pas d'être intouchable et invulnérable, mais plutôt de minimiser le risque et ses conséquences.

Afin de minimiser le risque, *_da_da_da* et *organichewn*, qui se considèrent tout deux comme des experts du darknet, ne se fient pas, ou peu, aux évaluations présentes sur les marchés, et utilisent des critères externes qui leur sont propres. Il s'agit là d'un comportement qui se retrouve sur des plateformes comme DNMAvengers, où usagers "experts" en matière de substances se retrouvent afin d'échanger savoirs et expériences, ou de mobiliser des prestataires externes, Energy Control étant le principal. La dernière ligne de protection consiste à tester soi même les substances achetées, en utilisant des kits chimiques changeant de couleur en fonction du produit avec lequel ils réagissent et permettant de détecter des produits de coupe potentiellement mortels.

En matière de minimisation des conséquences, notamment en cas de convocation par la police, les utilisateurs se reposent sur le fait qu'il existe de plus gros poissons à attraper. Le consensus à ce propos semble être que le but des gouvernements mondiaux n'est pas d'arrêter les petits consommateurs, qui n'en valent pas la peine et qui s'en voient donc protégés (BARRATT, 2011). Pour filer la métaphore aquatique, certains poissons faciles à attraper sont également présent dans l'océan des DNMs : il s'agit là des utilisateurs chiffrant leur message directement sur un DNM, voire pas du tout, ou de ceux n'utilisant pas d'OS sécurisé ni de VPN par exemple. S'il est impossible de garantir une sécurité totale, il est en revanche toujours possible d'être moins facile à retrouver que son voisin. L'autoprotection est une bonne chose quand elle

est bien intégrée par les utilisateurs, mais échoue souvent en pratique : seule une petite proportion des internautes la pratique de la bonne manière (PASQUALE, 2015), et les autres courent le risque de voir leurs activités dévoilées. Ce fut là l'une des conséquences de l'*Operation Bayonet*, après laquelle les “intelligence packages” discutés au cours du chapitre 3 montrèrent à quel point la plupart des acheteurs sur les DNMs ne prenaient pas les précautions les plus minimales.

5.3 Point de Passage Obligé ?

Nous avons postulé au début de ce travail que la confiance était un point de passage obligé pour les différents acteurs, mais il est apparu au fil des pages à quel point cette notion était mise à mal sur le darknet. Nous nous sommes également demandé comment il était possible pour les DNMs de fonctionner aussi bien, et là encore il est apparu que ceux-ci ne fonctionnaient pas si bien que cela : *exit scams*, arnaques et scandales en tout genre maculent la longue histoire de ces plateformes.

Là où pêcheurs, coquilles saint jacques et scientifiques (CALLON, 1986) n'avaient d'autre choix que de collaborer pour atteindre leurs objectifs, acheteurs, vendeurs et marchés peuvent utiliser toutes sortes de chemins détournés pour arriver à leurs fins. Si la confiance est un PPO, il s'agit donc plutôt d'un point de passage optimal qu'obligé : la confiance facilite le bon déroulement des affaires, mais son absence ne l'entrave pas plus que cela. Effectivement, malgré le succès indéniable de l'*Operation Bayonet* en matière de destruction de la confiance, Dream Market est encore témoin de centaines de ventes chaque jour, et les nombreux forums liés au sujet montrent que l'achat et la vente de substances en ligne ont encore de beaux jours devant eux, même si leur âge d'or est bel et bien passé.

La question de l'agir des acteurs est intéressante à soulever ici : Nooteboom (2006) postule que survient un moment où « je dois agir ici et maintenant ». Cela n'est pas le cas sur les DNMs, exception faite de quelques cas particuliers. Comment se fait-il que des centaines de milliers de personnes à travers le monde soient prêtes à prendre de tels risques pour se procurer des substances, action à priori totalement dispensable ? Malgré les efforts de plusieurs pays, malgré les revers subis par les différents acteurs, et malgré les risques encourus, les DNMs perdurent et sont utilisés de manière globale. Ces plateformes sont la preuve en action que les politiques de prohibition ne fonctionnent pas, et leurs enseignements pourraient être utilisés pour mettre en place de nouveaux moyens de lutter contre les addictions.

Pour conclure, les DNMs sont un rêve néolibéral devenu réalité : ne disposant d'aucun gouvernement central ou organisme de régulation, le système au sein duquel ils évoluent fonctionne pourtant correctement. La présence d'acteurs nuisibles est inévitable, mais les récentes affaires au sein de nos sociétés contemporaines (viande de cheval dans les lasagnes, lait contaminé, crise des *subprimes*, etc.) montrent qu'il s'agit là d'un

problème que l'on retrouve également "chez nous". L'avantage des DNMs réside dans leur résilience ainsi que leur rapidité d'adaptation. Ces deux caractéristiques en font des terrains de recherche tout à fait intéressants dans de nombreux domaines : sciences sociales comme ici, mais également psychologie sociale, sciences politiques ou encore économie comportementale.

A Entretiens

A.1 __da_da_da

Depuis quand utilises-tu le darknet pour acheter des substances ?

2012 ; Canna, LSD, MDMA, 2C-B, DMT

Combien de fois en as-tu achetées ?

Une petite vingtaine de fois

Est-ce que tu t'es déjà fait arnaquer par un vendeur (produit non envoyé, poids inférieur à ce qui était affiché, qualité moins bonne que prévue, etc.) ?

Pas que je me souviene. Par contre j'ai perdu de l'argent lors de la disparition de blackbank.¹

Est-ce que quand tu commandes, tu prends des mesures pour ne pas te faire arnaquer par le vendeur (lecture de recommandations, sélection de vendeur en fonction du nombre de transactions, etc.) ?

Oui. Avis ; nombre de transactions ; escrow ; qualité de la description. Je prends aussi sa clé PGP (qui sert d'identifiant unique d'un market à l'autre) et je la balance dans Grams Infodesk qui me ressort un agrégat de ses avis et transactions sur tous les markets.

Est-ce que tu as déjà eu des ennuis avec la police, en lien avec tes achats sur le darknet (produits interceptés par la douane, convocation au poste, etc.) ?

Jamais

Est-ce que quand tu commandes, tu prends des mesures pour ne pas avoir d'ennuis avec la police (VPN, système d'exploitation sécurisé, faux nom/ fausse adresse, blanchiment de bitcoins, etc.) ?

J'utilise Tor Brower (j'évite les proxys du style tor2web). Je chiffre en PGP en local (utiliser le "chiffrement automatique" des markets nullifie l'intérêt de PGP). Le VPN ne sert à rien au-dessus de Tor quoi qu'en disent ses défenseurs. Mon OS n'est

1. N.B. : BlackBank Market, l'un de plus gros marchés lorsque le site était encore accessible, a brusquement cessé ses opérations en mai 2015. Même s'il s'agit probablement d'un *exit scam*, la raison de cet arrêt n'est pas connue.

pas particulièrement sécurisé, mais j'évite Windows. Vrai nom et adresse. Pas de blanchiment, mais c'est plutôt par flemme. J'ai tout entendu sur le blanchiment, je ne suis pas sûr que ça protège vraiment.

Par rapport à la police, j'estime que pour les quantités en jeu, je ne risque pratiquement rien.

Si tu avais l'habitude d'acheter "dans la rue", quel moyen trouves-tu supérieur (selon tes critères à toi) entre l'achat "dans la rue" et sur le darknet ?

Je n'ai jamais acheté dans la rue. Mais je vois plusieurs avantages pour le darknet :

Concurrence entre vendeurs encouragée, transparence sur les prix, pas de prix "à la tête"

La description, les avis et la réputation du vendeur permettent d'avoir une idée assez précise de ce qu'on consomme. Pour le canna, pas d'incertitude sur la variété. Pour les produits, on peut raisonnablement supposer que la substance est celle annoncée. En plus, c'est assez facile de trouver des retours d'expérience, des retours de test kits ou de tests en labo, parfois même directement sur la page de l'annonce.

Sécurité physique

Choix large, accès à des produits exotiques

Sur une échelle de 1 à 10 (1 = débutant, 10 = expert), tu te placerais à combien, en termes de connaissance du darknet ? Je sais que cette question est très vague, mais on pourrait imaginer que 1 correspondrait à quelqu'un qui suit un tutoriel étape par étape pour commander de la drogue sans vraiment comprendre, et 10 quelqu'un qui prend absolument toutes les précautions nécessaires pour ne pas se faire arrêter/arnaquer, et qui maîtrise parfaitement les outils.

Je dirais 9, j'ai un background en infosec et je comprends très bien les mécanismes.

Je pense que le darknet en l'état est difficilement accessible à l'utilisateur lambda. Il faut comprendre l'anglais, appréhender des principes peu intuitifs comme PGP, utiliser les markets qui sont généralement peu ergonomiques, et c'est facile de se faire arnaquer.

Voilà ! :) n'hésite pas si tu veux en savoir plus

Pour en revenir à Grams, c'est le seul prestataire externe aux markets que tu utilises ? Pas de /r/darknetmarkets du temps où ça existait encore, ou dnmavengers/dread ?

Sisi tout à fait, je traînais beaucoup sur /r/darknetmarkets et puis je google toujours le nom du vendeur et/ou le nom du cachet de MD par exemple.

J'ai essayé dnmavengers/dread rapidement après la fin de /r/darknetmarkets mais j'ai eu du mal à trouver des infos. Petite communauté et moteurs de recherche inefficaces, si je me souviens bien.

J'oubliais, je suis fan du multisig (le darknet est un excellent cas d'utilisation pour ça) et je l'utilise quand c'est possible. Malheureusement, c'est rare de trouver une combinaison produit/pays/multisig convenable.

C'est aussi généralement peu intuitif de faire une transaction en multisig, quoiqu'il existe peut-être des wallets qui le facilitent.

Pour les pays d'expédition :

LSD/blotters : n'importe quel pays, c'est pratiquement indétectable

Canna et cachets : France quand c'est possible (surtout pour le canna qui est relativement facile à trouver par les douanes), sinon Allemagne. J'évite les pays-bas, le pays est flaggé.

A.2 pouetpouet123456

Depuis quand utilises-tu le darknet pour acheter des substances ?

J'ai commandé la première fois mi 2016, j'ai commandé 2-3 fois puis j'ai arrêté, et la depuis quelques temps je m'y suis remis.

Combien de fois en as-tu achetées ?

5-6 fois pour le moment.

Est-ce que tu t'es déjà fait arnaquer par un vendeur (produit non envoyé, poids inférieur à ce qui était affiché, qualité moins bonne que prévue, etc.) ?

Oui une fois, c'est pour ça que j'avais arrêté, mais c'était en parti ma faute. Je n'avais pas reçu mon colis, il y a un système appelé "Escrow" qui garde ton argent sur un wallet pendant un temps défini, tu dois recevoir la commande avant la fin de ce temps, si tu ne reçois rien, tu contactes le vendeur, s'il te répond pas tu vois avec le site et tu peux récupérer ton argent. Le truc c'est que j'avais oublié de recontacter le vendeur.

Est-ce que quand tu commandes, tu prends des mesures pour ne pas te faire arnaquer par le vendeur (lecture de recommandations, sélection de vendeur en fonction du nombre de transactions, etc.) ?

Oui, je regarde les commentaires des acheteurs, et surtout si le vendeur est connu et a déjà eu beaucoup de client.

Est-ce que tu as déjà eu des ennuis avec la police, en lien avec tes achats sur le darknet (produits interceptés par la douane, convocation au poste, etc.) ?

Non pas du tout.

Est-ce que quand tu commandes, tu prends des mesures pour ne pas avoir d'ennuis avec la police (VPN, système d'exploitation sécurisé, faux nom/fausse adresse, blanchiment de bitcoins, etc.) ?

Il faut utiliser Tor, donc VPN obligatoire. J'utilise mon vrai nom et ma vraie adresse, pour les bitcoin je les achète sur coinbase, je les transfère sur un wallet perso et ensuite sur le site de vente. Jm'en fait pas trop pour la sécurité, je commande pas de grosses quantités.

Si tu avais l'habitude d'acheter "dans la rue", quel moyen trouves-tu supérieur (selon tes critères à toi) entre l'achat "dans la rue" et sur le darknet ?

Le darknet est pratique, tu donnes ton adresse (par envoi chiffré), l'argent, et 3 jours plus tard t'as une enveloppe dans ta boîte aux lettres. Dans la rue c'est plus compliqué, faut trouver les bonnes personnes pour avoir des bons prix et des bons produits. Quand t'arrives dans une ville que tu ne connais pas c'est compliqué. Sinon niveau prix, ça dépend ce que tu prends, la weed est plus chère sur le darknet que IRL, et le shit c'est aussi chère voire moins chère que ce que tu trouves dans la rue.

Sur une échelle de 1 à 10 (1 = débutant, 10 = expert), tu te placerais à combien, en termes de connaissance du darknet ? Je sais que cette question est très vague, mais on pourrait imaginer que 1 correspondrait à quelqu'un qui suit un tutoriel étape par étape pour commander de la drogue sans vraiment comprendre, et 10 quelqu'un qui prend absolument toutes les précautions nécessaires pour ne pas se faire arrêter/arnaquer, et qui maîtrise parfaitement les outils.

Je dirais 6, je fais pas particulièrement attention à ma sécurité, enfin un minimum quand même, mais je sais trouver des vendeurs facilement et faire une commande aussi.

9. Et du coup quand tu dis que tu regardes les commentaires des acheteurs c'est seulement sur les marchés ?

Ouai.

Ou bien tu te sers aussi des plateformes externes (comme /r/darknetmarkets (qui n'existe plus), dread, dnnavengers, etc.) pour avoir des analyses un peu plus poussées ?

J'ai cherché un peu, mais y a pas beaucoup de review pour les vendeurs français vu que je ne commande qu'en France.

A.3 *organichewn*

Depuis quand utilises-tu le darknet pour acheter des substances ?

3-4 ans environ, pour acheter principalement de la md et du speed.

Combien de fois en as-tu achetées ?

Une trentaine de fois, en comptant les fois où j'ai commandé pour des amis.

Est-ce que tu t'es déjà fait arnaquer par un vendeur (produit non envoyé, poids inférieur à ce qui était affiché, qualité moins bonne que prévue, etc.) ?

Oui, pas mal de fois, et c'était à chaque fois des fois où j'avais FE et où je n'ai jamais reçu le produit. J'ai aussi eu des cas où la quantité était un peu inférieure (mais de peu), ou la qualité pas top. Mais je ne considère pas vraiment ça comme des arnaques.

Par contre il m'est aussi arrivé d'avoir des erreurs en ma faveur. J'avais commandé il y a quelques années 0.2g de 2C-B, et j'en ai reçu 2g. Et avec de la md aussi, commandé 5g et reçu 15.

Est-ce que quand tu commandes, tu prends des mesures pour ne pas te faire arnaquer par le vendeur (lecture de recommandations, sélection de vendeur en fonction du nombre de transactions, etc.) ?

Je choisis un vendeur qui a beaucoup de transactions et de feedbacks positifs. Je ne lis pas les critiques sur les marchés ou ailleurs, parce que rien ne prouve qu'elles sont vraies. Et je ne FE jamais. En général je commence par acheter un échantillon, pour vérifier la stealth du vendeur et voir si effectivement je reçois quelque chose. Si tout joue je passe à une vraie commande.

Est-ce que tu as déjà eu des ennuis avec la police, en lien avec tes achats sur le darknet (produits interceptés par la douane, convocation au poste, etc.) ?

J'ai eu un colis intercepté par la douane une fois. J'ai dû aller à la brigade des stupéfiants pour m'expliquer, et j'ai fini par passer devant un juge qui m'a mis une petite amende. J'avais commandé à un vendeur hollandais, ce qui était une erreur puisque le pays est surveillé.

Est-ce que quand tu commandes, tu prends des mesures pour ne pas avoir d'ennuis avec la police (VPN, système d'exploitation sécurisé, faux nom/fausse adresse, blanchiment de bitcoins, etc.) ?

Je ne commande plus à des vendeurs hollandais, et je ne commande jamais de pilules parce que ça se détecte facilement en touchant l'enveloppe. J'utilise un VPN et je n'utilise pas mon vrai nom. J'ai essayé TAILS mais c'est trop chiant à utiliser. Pas de blanchiment de bitcoins, de toute façon ça n'est pas totalement anonyme.

Si tu avais l'habitude d'acheter "dans la rue", quel moyen trouves-tu supérieur (selon tes critères à toi) entre l'achat "dans la rue" et sur le darknet ?

Je n'avais pas l'habitude d'acheter dans la rue. Mais le darknet est clairement supérieur. Les prix sont divisés par 10 pour certains trucs, et la qualité est meilleure d'après ce

que j'ai pu lire. En plus je n'ai pas à interagir avec qui que ce soit, je peux commander tranquillement depuis chez moi.

Sur une échelle de 1 à 10 (1 = débutant, 10 = expert), tu te placerais à combien, en termes de connaissance du darknet ? Je sais que cette question est très vague, mais on pourrait imaginer que 1 correspondrait à quelqu'un qui suit un tutoriel étape par étape pour commander de la drogue sans vraiment comprendre, et 10 quelqu'un qui prend absolument toutes les précautions nécessaires pour ne pas se faire arrêter/arnaquer, et qui maîtrise parfaitement les outils.

En tout cas 8 ou plus. A mon avis le 10 n'est pas possible, surtout quand on voit que des mecs comme DPR ont laissé des traces partout. Le risque est aussi de penser qu'on est à 10 et de commencer à faire des erreurs. Donc 8 ou 9 en ce qui me concerne.

Références

- AKERLOF, George A (1978). « The market for “lemons” : Quality uncertainty and the market mechanism ». In : *Uncertainty in Economics*. Elsevier, p. 235-251.
- ALPCAN, Tansu et al. (2010). « A game theoretic model for digital identity and trust in online communities ». In : *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. ACM, p. 341-344.
- AMBLEE, Naveen et Tung BUI (2008). « Can brand reputation improve the odds of being reviewed on-line ? » In : *International Journal of Electronic Commerce* 12.3, p. 11-28.
- BANCROFT, Angus et Peter Scott REID (2016). « Concepts of illicit drug quality among darknet market users : Purity, embodied experience, craft and chemical knowledge ». In : *International Journal of Drug Policy* 35, p. 42-49.
- BARRATT, Monica J (2011). « Discussing illicit drugs in public internet forums : Visibility, stigma, and pseudonymity ». In : *Proceedings of the 5th International Conference on Communities and Technologies*. ACM, p. 159-168.
- BEARMAN, Joshua (avr. 2015). *The Rise & Fall of Silk Road*. WIRED. URL : <https://www.wired.com/2015/04/silk-road-1/>.
- BEAUDE, Boris (2012). *Internet : Changer l'espace, changer la société*. FYP éditions.
- BEAUVISAGE, Thomas, Jean-Samuel BEUSCART, Vincent CARDON et al. (2013). « Notes et avis des consommateurs sur le web ». In : *Réseaux* 1, p. 131-161.
- BEAUVISAGE, Thomas, Jean-Samuel BEUSCART, Kevin MELLET et al. (2014). « Une démocratisation du marché ? » In : *Réseaux* 1, p. 163-204.
- BEAUVISAGE, Thomas et Kevin MELLET (2016). « Travailleurs du like, faussaires de l'e-réputation ». In : *Réseaux* 3, p. 69-108.
- BOTSMAN, Rachel (2017). *Who Can You Trust ? : How Technology Brought Us Together—and Why It Could Drive Us Apart*. Penguin UK.
- CALLON, Michel (1986). « Éléments pour une sociologie de la traduction : la domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc ». In : *L'Année sociologique (1940/1948-)* 36, p. 169-208.
- CAMP, J. L. (2004). « Digital identity ». In : *IEEE Technology and Society Magazine* 23.3, p. 34-41.
- DE FILIPPI, Primavera et Benjamin LOVELUCK (2016). « The invisible politics of Bitcoin : governance crisis of a decentralized infrastructure ». In : *Internet Policy Review* 5.4.

- DEUTSCH, Morton (1958). « Trust and suspicion ». In : *Journal of conflict resolution* 2.4, p. 265-279.
- GOFFMAN, Erving (1974). *Frame analysis : An essay on the organization of experience*. Harvard University Press.
- GREIF, Avner (1989). « Reputation and coalitions in medieval trade : evidence on the Maghribi traders ». In : *The journal of economic history* 49.4, p. 857-882.
- HABER, Stéphane (2006). « Confiance et lien interpersonnel de Husserl à Luhmann ». In : *Les moments de la confiance*. Sous la dir. d'Albert OGIEN et Louis QUÉRÉ. Economica.
- HABER, Stuart et W Scott STORNETTA (1990). « How to time-stamp a digital document ». In : *Conference on the Theory and Application of Cryptography*. Springer, p. 437-455.
- HENSLIN, James M (1968). « Trust and the cab driver ». In : *Sociology and everyday life*, p. 138-158.
- HOLLAND, Rick, Rafael AMADO et Michael MARRIOTT (2018). *Seize and Desist ? The State of Cybercrime in the Post-AlphaBay and Hansa Age*. URL : <https://info.digitalshadows.com/rs/457-XEY-671/images/SeizeandDesist.pdf>.
- JACQUET, Édouard (2015). « Le «prêt payant». Les paradoxes de l'économie collaborative ». In : *Réseaux* 2, p. 99-120.
- LECOMTE, Romain (2010). « L'anonymat comme "art de résistance". Le cas du cyberspace tunisien ». In : *Terminal* 105, p. 55-68.
- LUHMANN, Niklas (2006a). « Confiance et familiarité. Problèmes et alternatives ». In : *Les moments de la confiance*. Sous la dir. d'Albert OGIEN et Louis QUÉRÉ. Economica.
- (2006b). *La confiance : un mécanisme de réduction de la complexité sociale*. Economica.
- MARKOFF, John (2005). *What the Dormouse Said : How the Sixties Counterculture Shaped the Personal Computer Industry*. Penguin.
- NAKAMOTO, Satoshi (2008). *Bitcoin : A peer-to-peer electronic cash system*. URL : <https://bitcoin.org/bitcoin.pdf>.
- NOOTEBOOM, Bart (2006). « Apprendre à faire confiance ». In : *Les moments de la confiance*. Sous la dir. d'Albert OGIEN et Louis QUÉRÉ. Economica.
- OGIEN, Albert et Louis QUÉRÉ (2006). *Les moments de la confiance*. Economica.
- PARSONS, Malcolm et Peter EBINGER (1968). « Interaction : I. Social Interaction ». In : *The international encyclopedia of the social sciences*. Citeseer.
- PASQUALE, Franck (2015). *Black Box Society. Les algorithmes secrets qui contrôlent l'économie et l'information*. FYP editions.
- PILISUK, Marc et Paul SKOLNICK (1968). « Inducing trust : a test of the Osgood proposal. » In : *Journal of Personality and Social Psychology* 8.2p1, p. 121.
- ROUVROY, Antoinette et Thomas BERNS (2013). « Gouvernamentalité algorithmique et perspectives d'émancipation ». In : *Réseaux* 1, p. 163-196.

-
- SHEETS-JOHNSTONE, Maxine (2006). « Sur la nature de la confiance ». In : *Les moments de la confiance*. Sous la dir. d'Albert OGIEN et Louis QUÉRÉ. Economica.
- STRUB, Peter J et TB PRIEST (1976). « Two patterns of establishing trust : The marijuana user ». In : *Sociological Focus* 9.4, p. 399-411.
- VANDERSTRAETEN, Raf (2002). « Parsons, Luhmann and the theorem of double contingency ». In : *Journal of Classical Sociology* 2.1, p. 77-92.
- YAN, Zheng et Silke HOLTMANNS (2008). « Trust modeling and management : from social trust to digital trust ». In : *IGI Global*, p. 290-323.