Considérations juridiques sur PrivateSend

Sommaire

Le fonctionnement des transactions Dash est identique à celui de Bitcoin. En conséquence, pour les questions de conformité légale et réglementaire, Dash peut et doit être traité de la même manière que Bitcoin.

Vue d'ensemble

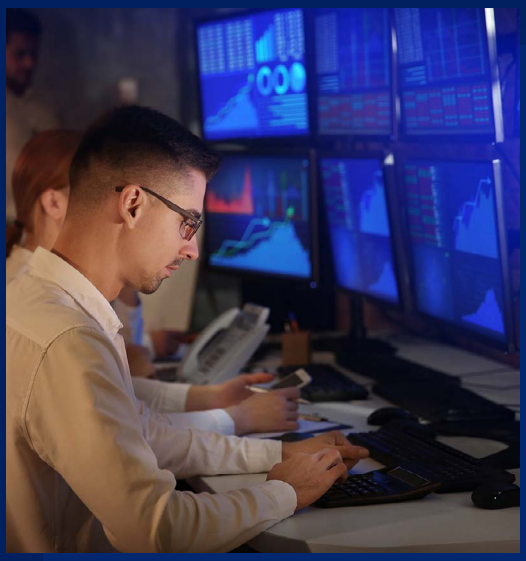
À mesure que les marchés cryptomonétaires ont mûri et sont devenus plus accessibles au grand public, les régulateurs de beaucoup de juridictions se sont interrogés sur la possibilité que les cryptomonnaies soient utilisées pour faciliter les activités illégales, parmi lesquelles le blanchiment d'argent. Une des réactions habituelles des corps législatifs et des instances exécutives est d'essayer de contraindre les plateformes de change et les autres acteurs du marché à ne pas intégrer les cryptomonnaies réputées être "dédiées à la confidentialité", sur la supposition que ces cryptomonnaies seraient celles qui auraient la préférence des délinquants et des criminels. Cependant, jusqu'ici, les interdictions proposées semblent se faire surtout en fonction de la réputation de telle ou telle cryptomonnaie, plutôt que sur des données techniques factuelles.

Dash, souvent étiqueté par les médias comme "dédié à la confidentialité", est parfois inclus dans les "listes de bannissement" proposées. Il s'agit là d'une classification inexacte pour Dash, aussi bien du point de vue réglementaire que légal. Ce document démontre en quoi le fonctionnement des transactions Dash est, en fait, identique à celui de Bitcoin. Il montre donc que Dash, sur les questions de conformité légale et réglementaire, peut et doit être traité de la même façon que Bitcoin.

Cela ne signifie pas que les portefeuilles Dash ne proposent pas à leurs utilisateurs une meilleure confidentialité. De manière générale, les fonctions de confidentialité et d'anonymat ne sont pas binaires, mais constituent un spectre. Ce spectre va de l'occultation complète des transactions (dans laquelle les adresses et les montants sont complètement masqués aux observateurs tiers) à des transactions complètement transparentes, en passant par l'occultation facultative des transactions. Par exemple, avec ZCash, les adresses occultées ne sont pas visibles et les transactions entre adresses occultées ne révèlent aucune des adresses, pas plus que le montant de la transaction ou le contenu chiffré de la notification. Par contraste, toutes les transactions Dash sont complètement transparentes et auditables car elles sont identiques à Bitcoin (sur lequel Dash se base), y compris pour les montants et les adresses impliquées dans chaque transaction. Comme nous allons le démontrer, les fonctions de confidentialité de Dash sont d'une nature presque identique aux technologies de confidentialité qui sont actuellement utilisables par les utilisateurs Bitcoin.

Dash, catégorisé correctement, se définit comme une monnaie numérique dédiée aux paiements et basée sur Bitcoin. Dash est une blockchain publique avec des fonctions de confidentialité supplémentaires disponibles dans son portefeuille logiciel pour ordinateur. Dash n'est pas optimisé en premier lieu pour une confidentialité maximale, ce qui impliquerait l'utilisation de technologies entraînant des inconvénients substantiels quant à la scalabilité, la rapidité, le coût des transactions et l'expérience utilisateur. Par exemple, beaucoup des cryptomonnaies optimisées pour une confidentialité maximale emploient des technologies qui les empêchent d'être utilisées sur des appareils mobiles, en raison de besoins importants de stockage et de puissance de calcul. Dash, au contraire, fait un arbitrage entre les différents besoins de l'utilisateur en plus de la confidentialité : par exemple la vitesse, la fiabilité, la scalabilité, la sécurité et les frais de transaction. Dash ne doit pas être traité différemment d'autres réseaux cryptomonétaires présentant des caractéristiques similaires, et doit être considéré indépendamment de son image auprès des médias.

Image de Dash parmi les cryptomonnaies



Dash est l'objet de certains stéréotypes et il a souvent été étiqueté comme une monnaie "dédiée à la confidentialité" par les médias cryptomonétaires. Cette étiquette peut s'expliquer par l'histoire de Dash et par son objectif de départ : en effet, PrivateSend a été la première des fonctionnalités mises en place par les programmeurs initiaux. L'étiquette de "monnaie dédiée à la confidentialité" est désormais tout à fait obsolète, car le projet Dash se consacre depuis les quatre dernières années à améliorer la simplicité d'emploi des cryptomonnaies en général. Par exemple, Dash propose désormais des transactions instantanées et une sécurité supérieure à celle de Bitcoin. Dash se consacre aussi particulièrement à l'expérience utilisateur générale, dans le but de rendre la cryptomonnaie plus familière et accessible pour le grand public. La prochaine version majeure de Dash inaugurera les noms d'utilisateur, les listes de contacts et des possibilités de stockage de données afin de rendre les transactions plus simples et plus personnalisables.

Dash a été lancé en 2014 sous le nom d'Xcoin par le développeur Evan Duffield. Une des premières améliorations apportées par Duffield a été d'implémenter CoinJoin dans le portefeuille logiciel Dash pour ordinateur de bureau. CoinJoin est une technologie de combinaison en une seule transaction (ou série de transactions) des paiements émanant de nombreux expéditeurs, ce qui rend plus difficile pour des parties tierces de déterminer quel expéditeur a payé tel destinataire. Au contraire de beaucoup d'autres technologies de confidentialité, les transactions CoinJoin n'impliquent aucune modification du protocole Bitcoin. Toutes les transactions restent transparentes sur la blockchain, y compris les sources des fonds utilisés dans la transaction, les adresses de destination et les montants. En conséquence, ces transactions peuvent aisément être identifiées comme telles par tout observateur — dont les observateurs tiers — et analysées par des logiciels de conformité juridique.

La réputation de Dash a été sans aucun doute impactée par la décision de l'équipe fondatrice de valoriser la différence apportée par la fonctionnalité PrivateSend, début 2014, en rebaptisant Xcoin en "Darkcoin". À mesure que le projet continuait à croître et ajoutait de nouvelles fonctionnalités, telles que les transactions instantanées, la marque Darkcoin était un frein à l'adoption en raison des connotations négatives avec les "dark markets" sur Internet. Bien que le nom du réseau ait été changé en "Dash" début 2015, la stigmatisation du nom "Darkcoin" s'est révélée durable, en particulier chez les journalistes. L'histoire de Dash est sans aucun doute l'une des principales raisons pour lesquelles Dash continue à être perçu comme "dédié à la confidentialité". Cependant, l'histoire ne doit pas déterminer ce que peut être de nos jours le traitement juridique appliqué à Dash.

En parallèle, Bitcoin et d'autres projets majeurs ont amélioré leurs propres fonctionnalités de confidentialité en suivant des approches qui sont presque identiques à la fonctionnalité InstantSend de Dash, et en utilisant leurs propres versions de CoinJoin. Cette technologie est celle que Dash a utilisée dès 2014 pour améliorer la confidentialité des transactions. Même si l'implémentation de CoinJoin par Dash est plus rapide, plus simple et moins coûteuse que des options similaires proposées par des portefeuilles Bitcoin, il n'existe aucune différence légalement définissable dans les transactions qui en résultent, comme nous allons le démontrer. Les améliorations principales par rapport à Bitcoin (par ex. : simplicité d'emploi, rapidité, sécurité, coût) sont des attributs communs à toutes les transactions Dash par rapport à Bitcoin, et ne sont en aucun cas attribuables à l'implémentation que fait Dash de CoinJoin.

Comme mentionné ci-dessus, CoinJoin a été implémenté dans un certain nombre de portefeuilles, outils et protocoles, dans Bitcoin et d'autres projets dérivés de Bitcoin, parmi lesquels :

Joinmarket	Dark Wallet	CoinJumble	CoinMux
CoinShuffle++	Zero Link	Samurai Wallet	Wasabi Wallet
CashShuffle (portefeuille pour Bitcoin Cash)			

Beaucoup de ces options ont été disponibles dès 2015, un an seulement après le lancement de la fonction PrivateSend de Dash. De plus, il existe un certain nombre de services Bitcoin de tierce partie qui, contre une commission, fournissent aux utilisateurs des fonds Bitcoin mélangés par CoinJoin. Ces options étaient disponibles avant même que la fonction PrivateSend de Dash ne le soit (en 2014). Enfin, il existe un certain nombre de technologies similaires, telles que TumbleBit ou CoinSwap, qui proposent une confidentialité similaire, mais qui ne sont pas basées sur CoinJoin.

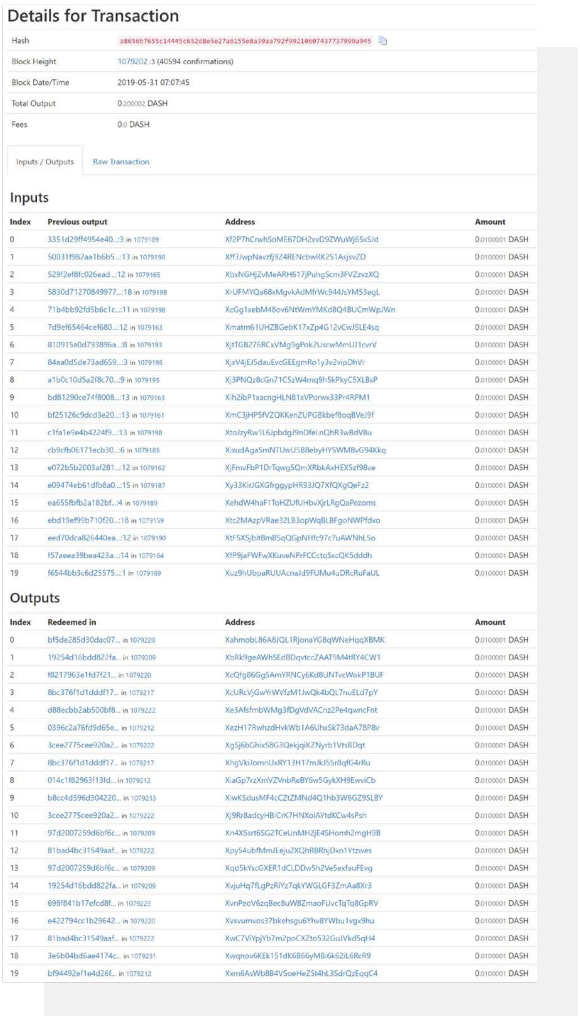
Également, de nouvelles technologies apparaissent qui visent à améliorer la confidentialité. Des améliorations significatives ont eu lieu concernant les implémentations CoinJoin de Bitcoin, telles que Chaumin CoinJoin : elles empêchent le serveur coordonnant la transaction entre utilisateurs de voir quelles adresses appartiennent à tel ou tel participant. De cette manière, même le serveur coordonnant la transaction ne manipule aucune information permettant une identification. Par ailleurs, de nouvelles méthodes de transaction hors chaîne ont été implémentées sur le réseau Bitcoin, parmi lesquelles le Lightning Network (LN). Les transactions LN individuelles ne sont pas du tout enregistrées sur la blockchain Bitcoin, seuls les participants aux transactions eux-mêmes peuvent les visualiser. Même au sein de LN, les serveurs de routage (également connus sous le nom de "nœuds") n'ont aucune connaissance des points de départ et d'arrivée d'une transaction.

Malgré leurs avancées technologiques, en accessibilité et en expérience utilisateur, les outils de confidentialité ont une utilisation qui reste assez limitée. De fait, les transactions CoinJoin constituent actuellement moins de 1% de toutes les transactions, que ce soit sur Bitcoin ou sur Dash, et l'adoption du Lightning Network évolue très lentement. Même si les taux d'utilisation étaient différents, établir une distinction juridique entre Bitcoin et Dash serait de moins en moins justifiable, étant donné le très grand nombre d'implémentations similaires existant désormais sur le marché. PrivateSend est simplement un nom de marque pour l'implémentation spécifique de CoinJoin que l'on trouve dans le portefeuille logiciel Dash pour ordinateur.

Des mécanismes identiques de transaction

De surcroît, les règles de transaction Bitcoin et Dash sont mutuellement inclusives.[1] Cela veut dire qu'une transaction Bitcoin valide serait tout aussi valide sur le réseau Dash, et vice versa. Cela signifie également qu'une transaction Bitcoin invalide serait invalide sur le réseau Dash, et inversement. Les adresses Dash et les transactions entre elles sont visibles publiquement sur la blockchain Dash, exactement de la même manière que les adresses Bitcoin le sont. En un mot, les règles qui définissent ce qu'est une transaction utilisateur valide sont complètement identiques. Il n'existe simplement aucun argument logique qui permettrait de traiter Dash autrement que Bitcoin dans une optique de conformité juridique et réglementaire.

De plus, Dash maintient une compatibilité parallèle avec Bitcoin, au fur et à mesure que des améliorations sont apportées au code source Bitcoin. Il en résulte qu'il n'existe aucune différence substantielle entre les transactions Dash et Bitcoin. De fait, les transactions PrivateSend peuvent être opérées sur le registre de transactions Bitcoin. Nous ne nous contentons pas de l'affirmer : nous en fournissons la preuve. Les deux transactions suivantes ont été menées respectivement sur les réseaux Dash et Bitcoin. Elles comprennent chacune 20 entrées et 20 sorties de 0,0100001 unité. Comme on peut le voir très clairement, la transaction Bitcoin n'est pas seulement similaire… Elle est *complètement identique*.[2]



Details for Transaction

Hash a8656b7655c14445c652d8e5e27a6155e8a39aa792f99210607437737999a945

Block Height 1079202 :3 (40594 confirmations)

Block Date/Time 2019-05-31 07:07:45

Total Output 0.200002 DASH

Fees 0.0 DASH

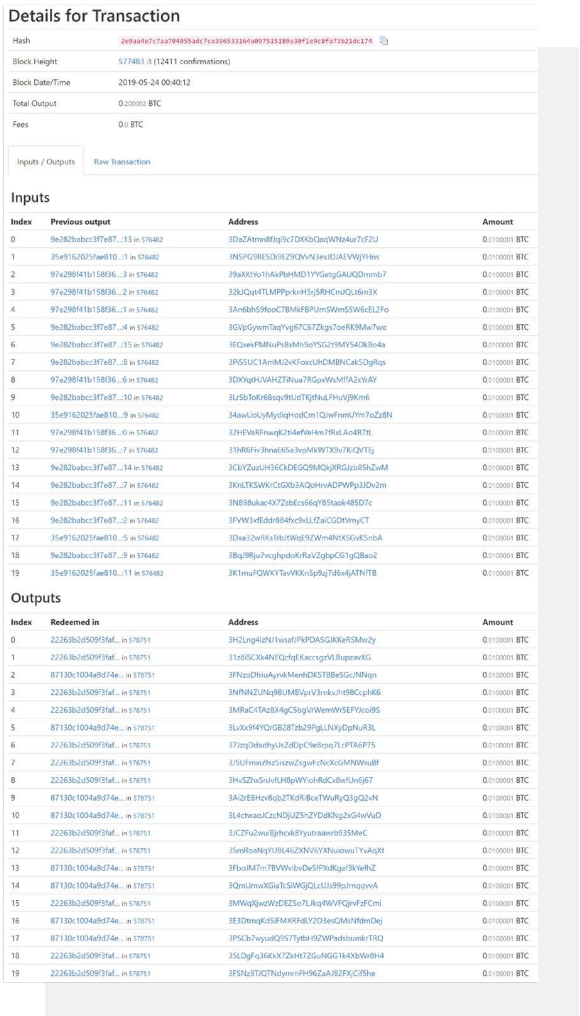
Inputs / Outputs | Raw Transaction

Inputs

Index	Previous output	Address	Amount
0	3351d29ff4954e40…:3 in 1079189	XfZP7hCrwhSoME67DH2svD9ZWuWj65xSid	0.0100001 DASH
1	50031f982aa1b6b5…:13 in 1079198	XffJJwpNavzfji9J4RENcbwRK251AsjsvZD	0.0100001 DASH
2	529f2ef8fc026ead…:12 in 1079165	XDxNGHjZvMeARH617jPuhqScn3FVZzvzXQ	0.0100001 DASH
3	5830d712708499777…:18 in 1079198	XrUFMYQa68xMgvkAdMfkWc94tJsYM53eqL	0.0100001 DASH
4	71b6bb92fd5b6c1c…:11 in 1079198	XcGg1xebM48ov6NtWmYMKd8Q4BUCmWpJWn	0.0100001 DASH
5	7d9ef65464ce1680…:12 in 1079163	Xmatm61UHZBGebK17xZp4Q12vCwJSLE4sq	0.0100001 DASH
6	810915a0d7938f96a…:8 in 1079193	XjtTGB27fiRCxVMgTgPok2UscwMmUJ1cnV	0.0100001 DASH
7	84ea0d5de73ad659…:3 in 1079198	XjxV4jEJ5daUEvcGEEgmRo1y3vZvipDhVr	0.0100001 DASH
8	a1b0c10d5a2f8c70…:9 in 1079195	Xj3PNQz8cGn71C5zW4mnq9h5kPkyC5XLBsP	0.0100001 DASH
9	bd81290ce74f8008…:13 in 1079163	Xih2ibP1xacngHLN81xVPorww33PrtRPM1	0.0100001 DASH
10	bf25126c9dcd3e20…:13 in 1079161	XmC3jHP5fVZQKKenZUPGBkbef8oqBVej9f	0.0100001 DASH
11	c1fa1e9e4b4224f9…:13 in 1079198	XtoJzyRw1L6jpbdgf9nDfeLnQhR3w8dV8u	0.0100001 DASH
12	cb9cfb06171ecb30…:6 in 1079185	XixudAga5mN1UwU5B8ebyHYSWM8vG94Kkq	0.0100001 DASH
13	e072b5b2003af281…:12 in 1079162	XjFmvFbP1DrTqwg5QmXRbkAxHEXSzf98ve	0.0100001 DASH
14	e09474eb61df5b8a0…:15 in 1079187	Xy33KirJGXGfrggypHR93JQ7XfQXgQeFz2	0.0100001 DASH
15	ea655fbfb2a182bf…:4 in 1079189	XehdW4haF1ToHZUfUHbvXjrLRgQaPezoms	0.0100001 DASH
16	ebd19ef99b710f20…:18 in 1079159	Xtc2MAzpVRae32LB3opWqBL8FgoNWPfdxo	0.0100001 DASH
17	eed70dca826440ea…:12 in 1079190	XtfSX5jbit8m85qQGpNHfc97c7uAWNhLSo	0.0100001 DASH
18	f57aeea39bea423a…:14 in 1079164	XtPSjaFWFwXKuveNrPrFCCcqSxcQK5dddh	0.0100001 DASH
19	f6544bb3c6d25575…:1 in 1079169	Xuz9hUbpaRUUAcnaJd3FUMu4uDRcRuFaUL	0.0100001 DASH

Outputs

Index	Redeemed in	Address	Amount
0	bf5de285d30dac07… in 1079220	XahmobL86A8JQL1RjonaYG8qWNeHqqXBMK	0.0100001 DASH
1	19254d16bdd822fa… in 1079209	XbRk9geAWhSEdBDqvtcc7AAT9M4tRY4CW1	0.0100001 DASH
2	f8217d63e1fd7f21… in 1079220	XcQfg86GgSAmYRNCy6Kd8tJNTvcWokP1BUF	0.0100001 DASH
3	8bc376f1d1dddf17… in 1079217	XcURcVjGwYvWVfzM1JwQk4bQL7nuELd7pY	0.0100001 DASH
4	d88ecbb23ab500bf8… in 1079222	Xe3AfsfmbWMg3fDgVdVACn22Pe4qwncFnt	0.0100001 DASH
5	0396c2a76fd9d65e… in 1079212	XezH17RwhzdHvkWb1A6UhxSk73daA78P8v	0.0100001 DASH
6	3cee2775cee920a2… in 1079222	XgSj6bGhixS8G3QekjqiKZNyrb1Vts8Dqt	0.0100001 DASH
7	8bc376f1d1dddf17… in 1079217	XhgVkiJomnUxRY13H17m4kf55r8qfG4rRu	0.0100001 DASH
8	014c1f82963f13fd… in 1079212	XiaGp7rzXmVZVnbRaBY6w5GykXH9EwviCb	0.0100001 DASH
9	b8cc4d596d304220… in 1079233	XiwKSdusMF4cCZtZMNd4Q1hb3W6GZ9SL8Y	0.0100001 DASH
10	3cee2775cee920a2… in 1079222	Xj9Rr8adcyHBiCrK7HNXoiAYtdKCwksPsh	0.0100001 DASH
11	97d200759d6bf6c… in 1079209	Xn4XSsrt6SG2TCeUnMH2jE4SHomh2mgH9B	0.0100001 DASH
12	81badd4bc31549aaf… in 1079222	Xpy54ubfMmuLejuzXQjNR8RhjDxn1Ytzwes	0.0100001 DASH
13	97d200725d6bf6c… in 1079209	Xqd5kYscGXER1dCLDDw5h2Ve5exfauFEvg	0.0100001 DASH
14	19254d16bdd822fa… in 1079209	XvjuHq7fLgPzRiYz7qkVWGLGF3ZmAa8Xr3	0.0100001 DASH
15	698f841b77efcd8f… in 1079223	XvnPeoV6zqBecBuW8ZmaoFUvcTqTq8GpRV	0.0100001 DASH
16	e42279cc1b29642… in 1079220	Xxvvumvos37bkehsgu6Yhv8YWbu1vgv9hu	0.0100001 DASH
17	81badd4bc31549aaf… in 1079222	XwC7ViVpjYb7m2poCXZto52GuiJVkd5qH4	0.0100001 DASH
18	3e6b04bd3ae4174c… in 1079231	XwgnovGKEk151dK6B6GyMBi6k52iL6RcR9	0.0100001 DASH
19	bf94492ef1e4d26f… in 1079212	Xxm6AsWbB4VSoeHeZSt4hL3SdrQzEqqC4	0.0100001 DASH



Details for Transaction

Hash 2e9aa4e7c7aa704055adc7ce396533164a0975151 89a30f1e9c8fa73b21dc174

Block Height 577483 :3 (12411 confirmations)

Block Date/Time 2019-05-24 00:40:12

Total Output 0.200002 BTC

Fees 0.0 BTC

Inputs / Outputs | Raw Transaction

Inputs

Index	Previous output	Address	Amount
0	9e282babcc3f7e87…:13 in 576482	3DsZAtmn8fJqi9c7DXKbQaqWNz4ur7cF2U	0.0100001 BTC
1	35e9162025fae810…:1 in 576482	3NSPG9RESOi9EZ9QVvN3exJDJAFVWjYHns	0.0100001 BTC
2	97a298f41b158f36…:3 in 576482	39aXKtYo1hAkPbHMD1YYGetgGAUQDnmnb7	0.0100001 BTC
3	97a298f41b158f36…:2 in 576482	32kJQqt4TLMPPprknH5rj5RHCmJQL16m3X	0.0100001 BTC
4	97a298f41b158f36…:1 in 576482	3An6bh59fooC7BMiFBPUmSWmSSW6cEL2Fo	0.0100001 BTC
5	9e282babcc3f7e87…:4 in 576482	3GVpGynmTaqYvg67C67Zkgs7oeRK9Mw7wo	0.0100001 BTC
6	9e282babcc3f7e87…:15 in 576482	3ECjxekPMNuPs8xMh9eYSCj2t9MY54D3c8o4a	0.0100001 BTC
7	9e282babcc3f7e87…:8 in 576482	3PjSSUC1AmMJ2vKFoxcUhDMBNCak5Dg8qs	0.0100001 BTC
8	97a298f41b158f36…:6 in 576482	3DXYqtHJVAHZTiNua78GpxWsMfFA2xYrAY	0.0100001 BTC
9	9e282babcc3f7e87…:10 in 576482	3LrSbToKr68sqv9tUdTKjtNuLFHuVj9Km6	0.0100001 BTC
10	35e9162025fae810…:9 in 576482	34awUoUyMydiqHodCm1QJwFnmUYm7oZz8N	0.0100001 BTC
11	97a298f41b158f36…:0 in 576482	32HEVaRFnwqK2ti4efVeHm7fRxLAn4R7tL	0.0100001 BTC
12	97a298f41b158f36…:7 in 576482	31hR6Fiv3hnaE65a3vpVkWTX9v7KiCjVTEj	0.0100001 BTC
13	9e282babcc3f7e87…:14 in 576482	3CbYZuzUH36CkDEGQ9MQkjRGJzlo8ShZwM	0.0100001 BTC
14	9e282babcc3f7e87…:7 in 576482	3KnLTKSWKrCtGXb3AQoHrvADPWPp3JDv2m	0.0100001 BTC
15	9e282babcc3f7e87…:11 in 576482	3N898ukac4X7ZtbEcs66qY85taok485D7c	0.0100001 BTC
16	9e282babcc3f7e87…:2 in 576482	3FVW3vfEddR884fxc9xLtZaiCGDtVmyCT	0.0100001 BTC
17	35e9162025fae810…:5 in 576482	3Dxa3zwYiKsTrbJtWqE9ZWm4NtXSGvK5nbA	0.0100001 BTC
18	9e282babcc3f7e87…:9 in 576482	3BqJ9Rju7vcghpdoKrRaVZgbpCG1gQBao2	0.0100001 BTC
19	35e9162025fae810…:11 in 576482	3K1muFQWKYTavVKKnSp8zj7d6x6jATNiTB	0.0100001 BTC

Outputs

Index	Redeemed in	Address	Amount
0	22263b2d509f3faf… in 576751	3H2Lng4izNJ1wsafJPkPDASGJKKeRSMw2y	0.0100001 BTC
1	22263b2d509f3faf… in 576751	31z8iSCXk4NECjcfqEKaccsgrVL8upzawXG	0.0100001 BTC
2	87130c1004a9d74e… in 576751	3FNzoDfriuAyrvkMenhDRSTBBe5GcfNNqn	0.0100001 BTC
3	22263b2d509f3faf… in 576751	3NfNNZUNq98UMBVprV3rnkvJtt9BCcpHK6	0.0100001 BTC
4	22263b2d509f3faf… in 576751	3MRaC4TAz8X4gC5bgVrWemWr5EPVJcoi9S	0.0100001 BTC
5	87130c1004a9d74e… in 576751	3LvXx9f4YQrGB287zb29RgLLNXyDpNuR3L	0.0100001 BTC
6	22263b2d509f3faf… in 576751	37JzqQddxhyUsZdDpC9e8rpq7LrPTA6P75	0.0100001 BTC
7	22263b2d509f3faf… in 576751	3J5UFmxu9sz5iszwZsgwFcNcXcGMNWsuBf	0.0100001 BTC
8	22263b2d509f3faf… in 576751	3HvSZhx5nJvfLH8pMYicNRdCx8wfUn6j67	0.0100001 BTC
9	87130c1004a9d74e… in 576751	3Ai2rEBHzv8qb2TKdRiBceTWuRyQ3gQ2vN	0.0100001 BTC
10	87130c1004a9d74e… in 576751	3L4ctwaoJCzcNDjUZSh2YDdKNg2xG4wVuD	0.0100001 BTC
11	22263b2d509f3faf… in 576751	3JCZFu2wuiBjrhcvk8Yyutraawrb935MeC	0.0100001 BTC
12	22263b2d509f3faf… in 576751	3SmRoaNqYU8L46ZXNV6YXNuiowu1YvAqXt	0.0100001 BTC
13	87130c1004a9d74e… in 576751	3FboJfM7m7BVWvbvDe5fPXdKgaf3kYefhZ	0.0100001 BTC
14	87130c1004a9d74e… in 576751	3QmUmwXGiaTcSiWGjQLcUJs99pJrnqqvvA	0.0100001 BTC
15	22263b2d509f3faf… in 576751	3MWqXjwzWzDEZSo7LJkq4WVFGjrvFzFCmi	0.0100001 BTC
16	87130c1004a9d74e… in 576751	3E3DtmqKd5iFMXRFdLY2D3esQMsNfdmDej	0.0100001 BTC
17	87130c1004a9d74e… in 576751	3PSCb7xyudQ3S7Tytbl49ZWPadsbumkrTRQ	0.0100001 BTC
18	22263b2d509f3faf… in 576751	3SLDgFqJGKsXTZkHt7ZGuNGG1tk4XbWrBH4	0.0100001 BTC
19	22263b2d509f3faf… in 576751	3FSNz9TJQTNdymmFH96ZaAJ82FXjCiF5hw	0.0100001 BTC

1 Techniquement, il existe quelques différences mineures, mais elles ne différencieraient pas Dash de Bitcoin d'un point de vue juridique. Par exemple, Dash utilise des "transactions spéciales" qui sont de nature non financière (par ex. pour stocker des données sur la blockchain). Ce type de transaction n'est pas traité par le réseau Bitcoin. Également, Bitcoin a mis en œuvre la technologie "Segregated witness", qui supprime une partie des données échangées pour réduire la quantité de données requises par une transaction. Cependant, aucune de ces différences mineures n'altère le format fondamental des transactions monétaires. Les deux réseaux répertorient les adresses d'entrée, les adresses de sortie et les montants, et ces informations sont consultables publiquement sur les deux.

2 https://chainz.cryptoid.info/dash/tx.dws?a8656b7655c14445c652d8e5e27a6155e8a39aa792f99210607437737999a945.htm
https://chainz.cryptoid.info/btc/tx.dws?2e9aa4e7c7aa704055adc7ce396533164a0975151 89a30f1e9c8fa73b21dc174.htm

Pourquoi la confidentialité est-elle importante ?

La confidentialité est indispensable pour toute activité entrepreneuriale, et elle est obligatoire dans le monde de la finance. Si les cryptomonnaies doivent être adoptées par le grand public et les entreprises, des outils de confidentialité sont nécessaires pour protéger les informations confidentielles (par ex. : combien sont payés vos employés, combien vous facturez vos services aux autres, quels sont les partis politiques que vous soutenez, etc.). Il existe de nombreuses raisons légitimes pour que les utilisateurs aient besoin de confidentialité, et en particulier celle que les blockchains publiques sont bien moins anonymes que l'argent liquide traditionnel ou même que les comptes bancaires, lesquels ne sont visibles que d'un petit nombre de tierces parties.

Notamment, la sécurité de l'utilisateur est d'une importance critique dans le domaine des cryptomonnaies. De nombreux cas d'agressions physiques, d'enlèvements, de rançons, de piratages et d'autres actes illégaux ont eu lieu contre des détenteurs importants de Bitcoin et d'autres cryptomonnaies. Et ces vols de fonds ne sont pas seulement le fait de criminels endurcis. Il est bien plus fréquent qu'ils soient le fait de membres de la famille, d'amis, de colocataires ou d'autres connaissances qui accèdent aux appareils des victimes pour leur subtiliser des fonds. La fonction PrivateSend de Dash aide à protéger les utilisateurs en empêchant que leurs transactions ou leurs soldes ne soient directement consultables sur la blockchain par des criminels qui souhaitent identifier les meilleures cibles, ou par des colocataires tentés par le vol après avoir identifié les adresses et les soldes de l'utilisateur. En conséquence, les fonctions de confidentialité sont absolument cruciales pour la sécurité de l'utilisateur.

La confidentialité est aussi une fonctionnalité nécessaire pour répondre aux obligations engendrées par certaines législations comme la GDPR (General Data Protection Regulation) dans l'Union européenne, ou encore le Consumer Privacy Act en Californie. Les législations dans le monde, telles que celles-ci, cherchent à trouver un équilibre entre protection des utilisateurs, pour des raisons de sécurité et de confidentialité, et contrôle de l'utilisation des cryptomonnaies à des fins illégales. La fonction PrivateSend de Dash offre aux utilisateurs la possibilité d'améliorer leur confidentialité, même si la blockchain reste publique.

Considérations sur la conformité juridique et réglementaire

Les plateformes de change et les autres passerelles vers les entités financières traditionnelles ont l'obligation d'appliquer de strictes conditions de conformité juridique, similaires à celles en vigueur concernant les dépôts et retraits d'argent liquide. Les plateformes conformes doivent suivre un ensemble de règles et de procédures pour attribuer une note de risque aux transactions, identifier les utilisateurs et signaler toute activité suspecte. Par leur nature même, les exigences de conformité juridique des transactions Dash sont les mêmes que celles des transactions Bitcoin. Les plateformes de change et les autres entreprises financières souhaitant intégrer Dash n'ont sans doute rien d'autre à faire que de dupliquer les règles et les procédures qu'elles utilisent déjà pour Bitcoin.

Beaucoup de plateformes de change s'appuient sur des services de tierce partie pour gérer leur programme de conformité juridique, plutôt que de concevoir elles-mêmes leur propre technologie. Ces services sont disponibles à la fois pour Bitcoin et Dash. BlockchainIntel et Coinfirm sont deux fournisseurs de service KYC/AML dont l'activité couvre à la fois les blockchains Bitcoin et Dash.

Il n'existe aucune différence entre Bitcoin et Dash du point de vue de la conformité juridique. Les mécanismes et protections actuellement utilisés dans l'écosystème Bitcoin pour la prévention du blanchiment d'argent sont applicables à Dash, sans changement. Les transactions PrivateSend peuvent être reconnues immédiatement en tant que telles sur la blockchain (tout comme les transactions CoinJoin dans Bitcoin), et toutes les transactions peuvent se voir attribuer une note de risque sur la base de trames de comportement, de proximité avec des adresses problématiques, de montant, ou de tout autre critère défini par la plateforme de change.

Conclusion

Malgré la classification fréquente, par la presse et les commentateurs du secteur, de Dash parmi les cryptomonnaies "dédiées à la confidentialité", il est important pour les régulateurs et les plateformes de change de comprendre que Dash est juridiquement et techniquement identique à Bitcoin. Il n'existe tout simplement aucune base juridique qui permettrait de traiter Dash différemment de Bitcoin en quoi que ce soit, en ce qui concerne les questions de conformité juridique et réglementaire. De fait, il serait injuste, anticoncurrentiel et potentiellement illégal pour les régulateurs de distinguer Dash du point de vue de la conformité juridique, puisque les deux mécanismes et formats de transaction sont identiques. Les lois devraient être rédigées de telle façon que les règles s'appliquent en fonction des caractéristiques et de la technologie des actifs numériques, et non pas du nom de telle ou telle blockchain — dont la technologie évolue avec le temps — sur la seule base de sa réputation, de sa marque ou de son image publique.

Dash Core Group demeure engagé en faveur de la confidentialité des utilisateurs et n'a pas cessé d'améliorer PrivateSend, notamment pour accroître sa vitesse. De plus, des avancées récentes dans nos technologies (LLMQ) rendent possible d'ajouter PrivateSend aux portefeuilles mobiles, ce que nous avons prévu de faire. À mesure qu'apparaîtront d'autres avancées dans les technologies de confidentialité, nous les étudierons toujours à travers le prisme de l'expérience utilisateur globale, car nous croyons que la confidentialité ne doit pas être proposée au détriment des autres fonctionnalités importantes d'un réseau de paiement. Le projet Dash a été pionnier dans la mise en œuvre de nouvelles technologies visant à offrir un bénéfice à la fois aux utilisateurs et aux vendeurs, et il continuera dans cette voie.

Toute plateforme de change, entreprise financière, corps législatif ou entité administrative souhaitant obtenir plus d'informations sur le traitement juridique et réglementaire de Dash peut obtenir des réponses à travers Dash Core Group, l'une des nombreuses entités au service du réseau Dash. Dash Core Group est une entreprise enregistrée au Delaware et dont le siège social est à Scottsdale, Arizona, États-Unis. Dash Core Group est la propriété intégrale du Dash DAO Irrevocable Trust établi au bénéfice des utilisateurs Dash. Dash Core Group collabore proactivement au nom du réseau avec des entités régulatrices telles que la SEC, l'Agence des Services financiers du Japon, la Commission européenne et le Parlement européen.

Dash Core Group peut être contacté
à l'adresse **support@dash.org**