

Prawne rozważania nt. PrivateSend

Podsumowanie

Reguły transakcyjne Dash są identyczne jak w przypadku Bitcoin i dlatego, na potrzeby zgodności z regulacjami, Dash może i powinien być traktowany identycznie jak Bitcoin.

Rozważania ogólne

Podczas gdy rynki kryptowalutowe dojrzały i stały się częścią maintream-u, regulatorzy w wielu jurysdykcjach obawiali się możliwości wykorzystania kryptowalut w celu ułatwienia nielegalnej działalności, w tym prania brudnych pieniędzy. Jedną z powszechnych reakcji organów legislacyjnych i organów ścigania jest próba postrzymania giełd i innych podmiotów rynku finansowego przed integracją tzw. kryptowalut „zorientowanych na prywatność”, opierając się na założeniu, iż owe kryptowaluty będą używane przez przestępców. Jednakże dotychczasowe próby zakazów wydają się opierać bardziej na reputacji danej marki niż na faktach technicznych.

Ponieważ Dash jest powszechnie określany w mediach jako kryptowaluta „zorientowana na prywatność”, niejednokrotnie był uwzględniany w proponowanych „listach zakazów”. Jest to niewłaściwe traktowanie Dash zarówno z punktu widzenia prawnego jak również z punktu widzenia istniejących regulacji finansowych. Niniejszy dokument dowodzi, że reguły transakcyjne stosowane w Dash są w rzeczywistości identyczne jak w Bitcoin, a zatem do celów prawnych i zgodności z regulacjami, Dash może i powinien być traktowany identycznie jak Bitcoin.

Nie oznacza to, że portfele Dash nie zapewniają użytkownikom prywatności. Funkcje prywatności i anonimowości nie są binarne, ale reprezentują raczej pewne spektrum funkcjonalności. Spektrum to obejmuje pełne zabezpieczenie transakcji (w których adresy i kwoty transakcji są całkowicie ukryte przed zewnętrznymi obserwatorami), opcjonalne zabezpieczenie transakcji i całkowicie przejrzyste transakcje. Przykładowo - w ZCash ekranowane adresy nie są widoczne, a transakcje między ekranowanymi adresami nie ujawniają ani adresu, ani kwoty transakcji ani zawartości zaszyfrowanego pola notatki. Natomiast transakcje Dash są całkowicie przejrzyste i możliwe do skontrolowania, identyczne jak w przypadku Bitcoin (na kodzie którego oparty jest Dash), włączając w to kwoty i adresy stron każdej transakcji. Funkcje prywatności Dash - jak pokażemy - są prawie identyczne z technologiami prywatności obecnie dostępnymi dla użytkowników Bitcoin.

Poprawna klasyfikacja Dash to cyfrowa waluta, oparta na kodzie Bitcoin i dedykowana płatnościom. Jest to publiczny blockchain z dodatkową funkcją prywatności w portfelu referencyjnym. Dash nie jest zoptymalizowany pod kątem zapewnienia całkowitej prywatności, gdyż wymagałoby użycia odmiennej technologii i znacznych kompromisów w zakresie skalowalności, szybkości, kosztów transakcji i ogólnej satysfakcji użytkownika. Przykładowo - wiele kryptowalut zoptymalizowanych pod kątem maksymalnej prywatności wykorzystuje technologie, które uniemożliwiają ich użycie na urządzeniach mobilnych ze względu na duże wymagania sprzętowe dotyczące przechowywania i przetwarzania danych. Dash natomiast koncentruje się na wielorakich potrzebach użytkowników poza prywatnością - są to przede wszystkim szybkość działania, niezawodność, skalowalność, bezpieczeństwo i koszt transakcji. Dash nie powinien być zatem traktowany inaczej niż inne sieci o podobnych atrybutach, niezależnie od tego, jak media przedstawiają projekt.

Postrzeganie Dash na rynku



Dash został stereotypowo oznaczony w mediach kryptowalutowych jako waluta „zorientowana na prywatność”. Postrzeganie to jest zakorzenione w historii waluty i początkowemu skupieniu się na aspekcie prywatności, gdy PrivateSend była pierwszą z udostępnionych funkcjonalności. Percepcja Dash jako waluty „zorientowanej na prywatność” jest obecnie bardzo nieaktualna, ponieważ w ciągu ostatnich czterech lat projekt został zorientowany na rzecz poprawy ogólnej użyteczności kryptowalut. Obecnie Dash oferuje bardzo szybkie transakcje i jeszcze większe bezpieczeństwo niż Bitcoin. Dash jest również bardzo zorientowany na poprawę wygody użytkowania portfela, tworząc kryptowalutę bardziej przyjazną i dostępną. Kolejna wersja protokołu wprowadzi funkcjonalności takie jak nazwy użytkowników, listy kontaktów i możliwości przechowywania danych w

blockchain, aby jeszcze bardziej usprawnić transakcje i ułatwić ich dostosowanie do zróżnicowanych potrzeb biznesowych.

Dash został utworzony w 2014 roku, jako projekt o nazwie „Xcoin”, przez programistę Evana Duffielda. Jednym z pierwszych ulepszeń, do których dążył Duffield było wdrożenie funkcjonalności CoinJoin w referencyjnym portfelu Dash QT. CoinJoin to technika łączenia wielu płatności od wielu podmiotów w jedną transakcję lub serię transakcji, aby utrudnić podmiotom zewnętrznym ustalenie, który nadawca zapłacił danemu odbiorcy lub odbiorcom. W przeciwieństwie do wielu innych rozwiązań w zakresie zapewnienia prywatności, transakcje CoinJoin nie wymagają modyfikacji protokołu. Wszystkie transakcje pozostają widoczne w łańcuchu bloków, włączając wszystkie źródła funduszy wykorzystane w transakcjach, adresy docelowe i kwoty. W związku z tym transakcje te mogą być łatwo zidentyfikowane przez każdego obserwatora - w tym zewnętrznych obserwatorów - i przeanalizowane przez oprogramowanie kontrolujące zgodność z istniejącymi regulacjami.

Na reputację Dash niewątpliwie wpłynęła decyzja zespołu założycieli o wykorzystaniu odmienności funkcjonalności PrivateSend i zmianie marki z "Xcoin" na „Darkcoin” na początku 2014 roku. W miarę rozwoju projektu i wprowadzania nowych funkcjonalności takich jak natychmiastowo potwierdzone transakcje, brand Darkcoin utrudniał adopcję z powodu negatywnych konotacji wywołanych przez powiązanie nazwy z rynkami dark markets. Choć nazwa projektu została zmieniona na „Dash” na początku roku 2015, piętno nazywania monety Darkcoin okazało się być trwałe, szczególnie wśród dziennikarzy. Fakt ten jest niewątpliwie jednym z głównych powodów dla których Dash nadal jest określany jako projekt „zorientowany na prywatność”. Jednak sama historia marki nie ma uzasadnienia dla prawnej klasyfikacji projektu.

W międzyczasie Bitcoin i inne wiodące projekty ulepszyły swoje własne funkcje prywatności, stosując podejścia niemal identyczne z PrivateSend, również wykorzystując własne wersje algorytmu CoinJoin. Należy pamiętać, iż jest to ta sama technologia, którą Dash wykorzystał w 2014 roku w celu zwiększenia prywatności transakcji. Pomimo, iż implementacja CoinJoin w Dash jest szybsza, łatwiejsza i tańsza w użyciu niż podobne opcje dostępne w portfelach Bitcoin, nie ma żadnych prawnie definiowalnych różnic w wynikowych transakcjach, co w niniejszym dokumencie wykażemy. Główne ulepszenia w porównaniu do Bitcoin (np. łatwość użycia, szybkość, bezpieczeństwo i niski koszt transferu) to atrybuty wspólne dla wszystkich transakcji Dash w porównaniu do Bitcoin i w żaden sposób nie można ich wiązać z implementacją CoinJoin w Dash.

Jak wspomniano powyżej, CoinJoin został zaimplementowany w wielu portfelach, narzędziach i protokołach w ramach Bitcoin lub w innych projektach utworzonych jako fork Bitcoin. Można tu wymienić:

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

Wiele z powyższych opcji jest dostępnych od 2015 r., zaledwie rok po udostępnieniu przez Dash funkcjonalności PrivateSend. Dodatkowo, istnieje wiele zewnętrznych serwisów dla Bitcoin oferujących miksery CoinJoin w zamian za dodatkowe opłaty. Te opcje działały jeszcze przed wprowadzeniem w 2014 roku funkcjonalności PrivateSend w Dash. Istnieje również wiele podobnych technologii, takich jak TumbleBit i CoinSwap, które oferują podobne usługi prywatności, ale nie są one oparte o algorytm CoinJoin.

Nowe technologie wciąż poprawiają usługi zapewniające prywatność. Wprowadzono znaczące ulepszenia we wdrożeniach CoinJoin dla Bitcoin, takie jak Chaumín CoinJoin, które uniemożliwiają serwerowi koordynującemu transakcję między użytkownikami sprawdzenie, które adresy należą do poszczególnych uczestników transakcji. W ten sposób nawet serwer koordynujący transakcję nie otrzymuje żadnych możliwych do zidentyfikowania informacji o użytkownikach. Ponadto w sieci Bitcoin zaimplementowano nowe metody transakcji poza łańcuchem - w tym Lightning Network (LN). Poszczególne transakcje LN nie są w ogóle rejestrowane w blockchainie Bitcoin a tylko uczestnicy transakcji są dla nich widoczni. Nawet w obrębie LN serwery routingu (tzw. „Węzły”) nie widzą punktów początkowych i końcowych transakcji.

Pomimo postępującego wyrafinowania, dostępności i lepszej użyteczności korzystanie z narzędzi do ochrony prywatności jest raczej marginalne. W rzeczywistości transakcje CoinJoin stanowią obecnie mniej niż 1% wszystkich transakcji zarówno dla Bitcoin jak i Dash a wdrażanie LN przebiega powoli. Nawet jeśli wskaźniki wykorzystania są różne, prawne rozróżnienie między Bitcoinem i Dashem jest nieuzasadnione, biorąc pod uwagę istnienie wielu podobnych implementacji. PrivateSend to po prostu nazwa marki dla konkretnej implementacji CoinJoin, znajdującej się w portfelu Dash QT.

Identyczne reguły transakcyjne

Ponadto zestaw reguł transakcji Bitcoin i Dash są wzajemnie powiązane.¹ Oznacza to, że poprawna transakcja Bitcoin byłaby także poprawna w sieci Dash i odwrotnie. Oznacza to również, że niepoprawna transakcja Bitcoin byłaby nieważna w sieci Dash i vice versa. Adresy Dash i transakcje między nimi są publicznie widoczne w blockchain Dash, dokładnie w taki sam sposób jak adresy Bitcoin są publicznie widoczne w blockchain Bitcoin. Krótko mówiąc, reguły określające prawidłową transakcję użytkownika są całkowicie identyczne w obu sieciach. Nie ma logicznego argumentu przemawiającego za tym, iż Dash powinien być traktowany inaczej niż Bitcoin ze względu na regulacyjne lub prawne.

Ponadto Dash utrzymuje zgodność własnego kodu z kodem Bitcoin, podążając za ulepszeniami wprowadzonymi w kodzie Bitcoin. W rezultacie nie ma istotnych różnic między transakcjami Dash i Bitcoin. W rzeczywistości transakcje PrivateSend można przeprowadzać w sieci Bitcoin. Nie tylko twierdzimy, że tak jest - przedstawiamy na to dowód. Dwie poniższe transakcje przeprowadzone odpowiednio w sieci Dash i Bitcoin. Obie mają po 20 wejść i 20 wyjść w ilości 0,0100001 każda. I jak widać, transakcja Bitcoin nie jest podobna... jest *całkowicie identyczna*.²

Details for Transaction

Hash: [2885967055c14451c632b69c74653568a39aa792599280874377179994945](#)

Block Height: 107502 (3 (40594 confirmations))

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

Total Output: 0.20000 DASH

Fees: 0 DASH

Inputs / Outputs: Raw Transaction

Inputs

Index	Previous output	Address	Amount
0	33514299f954e40...3 in 107189	XZP7HcWwS0mE67DHzvD2WwWj5SjId	0.0100001 DASH
1	50031F982aa1b6b5...13 in 107190	Xf31wPwKzcf9Z4REncwRkZ51AjsvZD	0.0100001 DASH
2	5292w8Bc025ead...12 in 107195	XbXGhZuMwARH617PuhgScm3FVzvxQZ	0.0100001 DASH
3	5830f7127084977...18 in 107198	XiUFVYQa8MgKvAUMWu3445YMS3eJL	0.0100001 DASH
4	71b4bb30f6936c1...11 in 107198	XcGtsebbM48w6NwMmXk8Q4BUcmWpWn	0.0100001 DASH
5	7d94954e4c6f80...12 in 107193	Xmatm61UHQZK6T1Zp6g12uGwLSLE4q	0.0100001 DASH
6	8109154d739896a...8 in 107193	XjTfCBZ7BRCvMg9gKt12cWmM21f0wVf	0.0100001 DASH
7	8aa0d55e73aa059...3 in 107198	Xjy4F5dauCEvEGmR9a7jYhvjyqDwV	0.0100001 DASH
8	a10c105a2b79c70...9 in 107195	Xj3PHQz8Gm71CSuW4mqz8k5PyCXLBpP	0.0100001 DASH
9	b0812500e749008...13 in 107193	XhZ2bP1xanghLhN81vPomw3P9fRPM1	0.0100001 DASH
10	b025126c3d0c3e20...13 in 107191	XmC3HPSVZQKKnZUGBkberBoqVUvFf	0.0100001 DASH
11	c19a1e94b4c22af9...13 in 107198	XtozyfWu1L6ipd9j9mDzicjR3wBw8VbU	0.0100001 DASH
12	c3b3e80e171c3c30...6 in 107185	Xixu4Ags5mNTLUsU5E8eBy1Y5WMB9G54kKq	0.0100001 DASH
13	e07265e2003af281...12 in 107192	XfFmF8P1D7qew5QmXRBkA4X5Sv98ve	0.0100001 DASH
14	e09474e81df0a0...15 in 107187	Xy3KjGjGqGgpphR3JQ7LqYQqFz2	0.0100001 DASH
15	e655f8b2a182b...4 in 107189	XehM4W4hF1TohZLULHwJvLqYQqFz2	0.0100001 DASH
16	ebd15e9271020...18 in 107199	Xtc2MAzP7Rae3ZL8jopW4BjLFqWpPzkw	0.0100001 DASH
17	eed703ca0e2440a...12 in 107190	Xf1SXSjyBf8eS0qGfH9F7CuAWNM5o	0.0100001 DASH
18	f57aea238aa423a...14 in 107144	XfP9jFmXUk0wvPRCC5u5cD5ddh	0.0100001 DASH
19	f6544b316d25575...1 in 107189	Xuz9Ulp9UUAa039FUM4DzURuRf4UL	0.0100001 DASH

Outputs

Index	Redeemed in	Address	Amount
0	bfd5e285f30da07... in 107920	Xahmobi86A8JQL1RjonaYQ6WV8Hqz8BMK	0.0100001 DASH
1	19254e11ebd482fa... in 107920	XoiRkEgeWHSdEgDqzctAA3fM48RY4CW1	0.0100001 DASH
2	f8217963a1fd7121... in 107920	XcQjg86G5AmYfNCy6K8JINtCwKpP18UF	0.0100001 DASH
3	8bc376f1dd4817... in 107921	XcLRLvG5wVwVfM1JavQk4QLTmELUfPj	0.0100001 DASH
4	d88c3b2ab500f8... in 107922	Xe3A4f8wMgHqDgVwVc2zPeFqumFnt	0.0100001 DASH
5	03962a78f59d65... in 107912	XezH177vhaHkV61A6U8j8KvA78P9v	0.0100001 DASH
6	3cew275ce920a2... in 107922	Xg5S6G8hK5CqGqkqZ7N9ybyVhUdDp	0.0100001 DASH
7	8bc376f1dd4817... in 107921	XhgVki0em0RyR3H17m5J55q9G54Rk	0.0100001 DASH
8	014c182863713d... in 107912	XaGp7xYmXZmR8eBwF6wGy4KH9EwvC3	0.0100001 DASH
9	b8c0d996d90420... in 107920	XiwK5du4fCz2M4H4Q1B83W5G29SLBY	0.0100001 DASH
10	3cew275ce920a2... in 107922	Xj9R8AdyH8C7H7N4vKwCw5Pn	0.0100001 DASH
11	97d200759860f6... in 107920	XoX4SereSG2CqUqMhJG4SHomhZmgH9B	0.0100001 DASH
12	81ba4bc31549aa... in 107922	Xpy4SubMmJugLQcR8BRR1DmV1tzvcs	0.0100001 DASH
13	97d200759860f6... in 107920	Xqz5Y5uXKER1dL2D5v5fZ3ZvXvEwFvEg	0.0100001 DASH
14	19254e11ebd482fa... in 107920	XqjHq7LqgR8Y7qVqVGLF3ZzAuA803	0.0100001 DASH
15	698f841b17efc08... in 107922	XmPecVoz8eBecW8ZmaoFJvTqTq8gRv	0.0100001 DASH
16	e427946c1b23642... in 107920	Xxwumv0s37k8q9y4WYBUyhgD9u	0.0100001 DASH
17	81ba4bc31549aa... in 107922	XwC7VW9v97mzoc3Zhe53G5uJvUdSg44	0.0100001 DASH
18	3a0504b30a4174c... in 107921	XwqnoV8EK1515t8689g9w4G43d46R9	0.0100001 DASH
19	b89492b71e4d26f... in 107912	Xm6A4Wb88Av5oHnzS4H35dQzEqc4	0.0100001 DASH

Details for Transaction

Hash: [2885967055c14451c632b69c74653568a39aa792599280874377179994945](#)

Block Height: 57483 (3 (12411 confirmations))

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

Total Output: 0.20000 BTC

Fees: 0 BTC

Inputs / Outputs: Raw Transaction

Inputs

Index	Previous output	Address	Amount
0	9e282abbc3f7e87...13 in 57682	3DzZArnn8f9c7DkXQacWzN4u7F2U	0.0100001 BTC
1	35e9162025fae810...1 in 57682	3N6PGR8S0RZ3QVnV8v3DIAEjVWYfIns	0.0100001 BTC
2	97a298f41b15836...3 in 57682	39AKX01o1h4kPLHMD1Y9e9GAUDmrm67	0.0100001 BTC
3	97a298f41b15836...2 in 57682	3ZU4Qt4tLMPpYkH5j5SRHcmQL6m3X	0.0100001 BTC
4	97a298f41b15836...1 in 57682	3An6b599oc7BmFRUm5WmSSW4eL2Fo	0.0100001 BTC
5	9e282abbc3f7e87...4 in 57682	3QjPqWymTa9vG3Z2qz4o8K9MwAvo	0.0100001 BTC
6	9e282abbc3f7e87...5 in 57682	3E5w4PMuK2v6Kw9C3Zqz4o8K9MwAvo	0.0100001 BTC
7	9e282abbc3f7e87...6 in 57682	3F55Uc1AnMk2v6Kw9C3Zqz4o8K9MwAvo	0.0100001 BTC
8	97a298f41b15836...4 in 57682	3D0Xq4V4H2Tnu47RQv4M5M142v4Af	0.0100001 BTC
9	9e282abbc3f7e87...10 in 57682	3U5bTol689q9U0Tq9N4PhuY9K6	0.0100001 BTC
10	35e9162025fae810...9 in 57682	34awL0LyM9d9H0dCm1QWfmmYm7oZ28N	0.0100001 BTC
11	97a298f41b15836...7 in 57682	31H86Fw3hna465a3pMwW1X9v7KQV1Ej	0.0100001 BTC
12	97a298f41b15836...7 in 57682	31H86Fw3hna465a3pMwW1X9v7KQV1Ej	0.0100001 BTC
13	9e282abbc3f7e87...14 in 57682	3C0VZu4LH36GDEQ2QmQjRg3a5hZuM	0.0100001 BTC
14	9e282abbc3f7e87...11 in 57682	3KxL2Wk3Wk3Cq3A3hV4dPwP3J3Dz2m	0.0100001 BTC
15	9e282abbc3f7e87...11 in 57682	3M988uac4K7Z6b3e66q8Stoak485D7c	0.0100001 BTC
16	9e282abbc3f7e87...12 in 57682	3FVW3v4d4884v4L4Z2aCGDmVCT	0.0100001 BTC
17	35e9162025fae810...5 in 57682	3Uwa32w5k5f8vW49J2bW4N3K5cV5n8A	0.0100001 BTC
18	9e282abbc3f7e87...8 in 57682	3Bq9j9v7u9gMk0kPaR2gbcCG1Q3a0z3	0.0100001 BTC
19	35e9162025fae810...11 in 57682	3K1muQWV7vVvK5G9j76wJATtB	0.0100001 BTC

Outputs

Index	Redeemed in	Address	Amount
0	2263b2u509f3af... in 578751	3H2Lmg4N1wsvfPKP0ASGJK6K85mVzy	0.0100001 BTC
1	2263b2u509f3af... in 578751	31z8SC04N4E9qfKacqzVlBuzwXG	0.0100001 BTC
2	87130c1004a9b74e... in 578751	3FNz8Dnu4yNkMeH3D2B85GcJN9n	0.0100001 BTC
3	2263b2u509f3af... in 578751	3MNNZUN4y8B8MvVur3NkHv188CpHkG	0.0100001 BTC
4	2263b2u509f3af... in 578751	3M8RcTAS4XgC3gVWwWm5EYfco9S	0.0100001 BTC
5	87130c1004a9b74e... in 578751	3Ux9f4YqYqG82b73PqL1XyDpN4R3L	0.0100001 BTC
6	2263b2u509f3af... in 578751	37zq3d4y1HkZd6f29C989qL7P4EPT5	0.0100001 BTC
7	2263b2u509f3af... in 578751	35Jfmu0z5c25v9p4cKvC6GMMWu8P	0.0100001 BTC
8	2263b2u509f3af... in 578751	3H5Z5u5vJbL7H4YvYkR4C4dLwJ6f7	0.0100001 BTC
9	87130c1004a9b74e... in 578751	3AaZ8Hv6bZ7K6R8c4WYU3q3Q2N	0.0100001 BTC
10	87130c1004a9b74e... in 578751	3LctwaoCzn4U52hZDl8ng24GmV4UD	0.0100001 BTC
11	2263b2u509f3af... in 578751	31CZfuzw5BjHk0z5YDl8ng24GmV4UD	0.0100001 BTC
12	2263b2u509f3af... in 578751	3F8w8q5YU8L46zXNvXUu0u1YukGt	0.0100001 BTC
13	87130c1004a9b74e... in 578751	3F8w8q5YU8L46zXNvXUu0u1YukGt	0.0100001 BTC
14	87130c1004a9b74e... in 578751	3QmWmW6iaT5SWGJQLu49m93qWvA	0.0100001 BTC
15	2263b2u509f3af... in 578751	3MWayjw8WfDEZ57Lkq4WVqjvFfCmI	0.0100001 BTC
16	87130c1004a9b74e... in 578751	3E3Dmg4Kz5M8Xf4V2Z9Lq4WVqjvFfCmI	0.0100001 BTC
17	87130c1004a9b74e... in 578751	3P5Cb7yyu0K927H4ZwZPd8m5mVtRQ	0.0100001 BTC
18	2263b2u509f3af... in 578751	35JdGf4304K4Z2H4Z2G4NG61W4XW8H4	0.0100001 BTC
19	2263b2u509f3af... in 578751	3F5Lq2TQ7N0ym7H8Z4A82fCF9w	0.0100001 BTC

¹ Technicznie istnieją pewne niewielkie różnice, które jednak nie różnicują Dash i Bitcoin z prawnego punktu widzenia. Przykładowo - Dash wprowadził „specjalne transakcje” o charakterze niefinansowym (np. do przechowywania danych w blockchain). Ten typ transakcji nie jest obsługiwany w sieci Bitcoin. Bitcoin z kolei wprowadził „segregated witness” - technologię, która usuwa część danych transakcji, aby zmniejszyć ilość danych w bloku. Żadna z tych drobnych różnic nie zmienia jednak podstawowego formatu transakcji walutowych. Obie sieci podają adresy wejściowe, adresy wyjściowe i kwoty oraz ujawniają te informacje publicznie.

² <https://chainz.cryptoid.info/dash/tx.dws?2a8656b7655c14445c652d8e5e27a6155e8a39aa792f99210607437737999a945.htm>
<https://chainz.cryptoid.info/btc/tx.dws?2e9aa4e7c7aa704055addc7ce396533164a097515189a30f1e9c8f73b21cd174.htm>

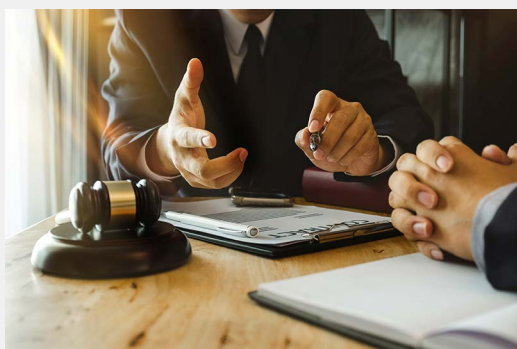
Dlaczego prywatność jest ważna?

Prywatność jest niezbędna do prowadzenia efektywnych operacji biznesowych. Jest również standardowym wymogiem w świecie finansów. Jeśli kryptowaluty mają zostać zaadoptowane przez prywatnych i instytucjonalnych użytkowników, potrzebne są narzędzia do ochrony prywatności w celu zabezpieczenia poufnych informacji (np. płace pracowników, opłaty za usługi dostawców zewnętrznych, dotacje na organizacje polityczne lub pozarządowe itd.). Istnieje wiele uzasadnionych powodów, dla których użytkownicy wymagają prywatności, szczególnie biorąc pod uwagę, że publiczne łańcuchy bloków są znacznie mniej anonimowe niż fizyczne środki płatnicze czy nawet konta bankowe, które są widoczne tylko dla ograniczonej liczby podmiotów.

Bezpieczeństwo użytkownika jest niezwykle ważne w odniesieniu do kryptowalut. Istnieje wiele przykładów napaści, porwań, żądania okupu, hakowania i innych nielegalnych działań przeciwko posiadaczom Bitcoinów i innych kryptowalut. I to nie tylko zahartowani przestępcy kradną kryptowalutowe fundusze. Znacznie częściej rejestrowano przypadki kradzieży przez członków rodziny, przyjaciół, współlokatorów czy innych znajomych, gdy wspólnie korzystano z dostępu do urządzeń ofiary. PrivateSend pomaga chronić użytkowników przed łatwym dostępem do historii ich transakcji lub sald w blockchain i zapobiega identyfikacji łatwych celów taku. Dlatego funkcje prywatności są niezwykle ważne również dla zapewnienia bezpieczeństwa użytkowników.

Prywatność to także funkcja niezbędna do spełnienia oczekiwań wynikających z przepisów o ochronie prywatności, takich jak Ogólne Rozporządzenie o Ochronie Danych Osobowych (GDPR) w Unii Europejskiej lub Ustawa o Ochronie Prywatności Konsumentów w Kalifornii. Przepisy te mają na celu zrównoważenie ochrony prywatności użytkowników z potrzebą zapobiegania wykorzystywaniu kryptowalut do nielegalnych celów. Funkcja PrivateSend zapewnia użytkownikom możliwość poprawy ich profilu prywatności, pomimo publicznego charakteru blockchajna.

Rozważania nt. zgodności z regulacjami



Giełdy kryptowalutowe i inne platformy dostępu do tradycyjnych podmiotów finansowych wymagają spełnienia rygorystycznych wymogów, podobnych do zasad mających zastosowanie do wpłat i wypłat gotówkowych. Regulowane giełdy zmuszone są do stworzenia całego zestawu zasad i procedur w celu oceny ryzyka transakcji, identyfikacji użytkowników i zgłaszania podejrzanych działań. Ze względu na swój charakter, wymagania zgodności z regulacjami dla transakcji Dash są identyczne z transakcjami Bitcoin. Giełdy lub inne firmy świadczące usługi finansowe, chcące zintegrować Dash, prawdopodobnie będą musiały jedynie

zreplikować istniejące już procedury i procesy już wykorzystywane w przypadku Bitcoin.

Wiele giełd używa zewnętrznych dostawców, którzy wspierają ich w zakresie zgodności z regulacjami, zamiast opracowywać własne technologie. Usługi takie są dostępne do obsługi zarówno Bitcoin, jak i Dash. Firmy BlockchainIntel i Coinfirm to dostawcy usług KYC / AML, którzy oferują usługi obejmujące zarówno blockchain Bitcoin, jak i Dash.

Różnice pomiędzy Bitcoin i Dash z punktu widzenia prawnego nie istnieją. Mechanizmy i zabezpieczenia stosowane obecnie w ekosystemie Bitcoin do zapobiegania praniu pieniędzy mają również zastosowanie do Dash. Transakcje PrivateSend można łatwo rozróżnić jako takie w blockchain (podobnie jak w przypadku transakcji Bitcoin CoinJoin), a wszystkie transakcje mogą być oceniane pod względem ryzyka na podstawie wzorców behawioralnych, bliskości do problematycznych adresów, wartości lub innych kryteriów określonych przez giełdę.

Wnioski końcowe

Pomimo często pojawiającej się klasyfikacji Dash jako kryptowaluty „zorientowanej na prywatność” w prasie i komentarzach branżowych, ważne jest aby regulatorzy i giełdy rozumieli, że Dash jest prawnie i technicznie identyczny z Bitcoin. Nie ma podstawy prawnej do traktowania Dash inaczej niż Bitcoin w celu określenia zgodności z istniejącymi regulacjami lub przepisami prawnymi. W rzeczywistości byłoby to działanie niesprawiedliwe, przeciwdziałające zrównoważonej konkurencji i potencjalnie nielegalne, gdyby organy regulacyjne traktowały Dash odmiennie z punktu widzenia prawnego, ponieważ w obu przypadkach zestawy reguł i form transakcji są identyczne. Przepisy powinny być napisane w sposób, który ustanawia reguły na podstawie atrybutów i technologii zasobu cyfrowego, a nie na podstawie nazwy, ewoluującego technicznie, blockchain czy w oparciu o rynkową reputację, markę lub po prostu (niejednokrotnie mylną) percepcję.

Dash Core Group pozostaje zainteresowaną ochroną prywatności użytkowników i wprowadza ulepszenia w PrivateSend, które znacznie zwiększyły szybkość tej funkcjonalności. Ostatnie ulepszenia technologiczne (LLMQ) umożliwiają dodanie PrivateSend do portfeli mobilnych, co planujemy zrobić w przyszłości. Kontynuując rozwój technologii ochrony prywatności, będziemy również wdrażać nowe rozwiązania pod kątem zwiększenia ogólnego zadowolenia użytkownika, sądząc, iż zapewnienie prywatności nie powinno odbywać się kosztem innych ważnych atrybutów sieci płatności. Projekt Dash był pionierem w poszukiwaniu nowych technologii, mających na celu zwiększenie użyteczności po stronie użytkownika i biznesu, i będzie kontynuować te działania.

Jakiegokolwiek giełdy, firmy świadczące usługi finansowe, organy ustawodawcze lub organy ścigania, poszukujące dodatkowych informacji na temat prawnego czy regulacyjnego traktowania Dash, mogą uzyskać wsparcie za pośrednictwem Dash Core Group, jednego z wielu podmiotów obsługujących sieć Dash. Dash Core Group to korporacja Delaware z siedzibą w Scottsdale, Arizona, USA. Dash Core Group jest w 100% własnością Dash DAO Irrevocable Trust. Dash Core Group w imieniu sieci aktywnie współpracuje z organami regulacyjnymi, takimi jak SEC, Japan Financial Services Agency, Komisja UE i Parlament UE.



Dash Core Group jest dostępny
pod adresem mailowym
support@dash.org