

Czerwiec 2019

Zcash (ZEC) -RAPORT

Rozwiązując zagadkę prywatności
kryptowalut



Autor: stokarz

Nadchodzi zmierzch ery bezpieczeństwa publicznego. Wielki Brat nie tylko patrzy, lecz również rozsiadł się na dobre, przeciągnął i rozpoczął aktywne działanie w celu realizacji swojego planu. Kiedy opinia publiczna debatuje nad coraz to nowymi, niecierpiącymi zwłoki sprawami, dziesiątki państw z chęcią dokonują zakupu technologii kontroli społecznej, made in China. Dziesiątki bilionów dolarów, jakie zostały dotąd przeznaczone na ten cel przez Chiński rząd, zdają się nie iść w błoto. Technologia kontroli obywateli stała się faktem i od kilkunastu miesięcy testowana jest w kilkunastu państwach na świecie. Nawet jeśli nie zainteresuje cię milion obywateli chińskich¹, z urodzenia będących muzułmanami, przetrzymywanych w obozach rodem z najczarniejszych koszmarów II wojny światowej, twoją uwagę powinien chociaż przykuć niedługo gotowy system rankingu społecznego, przywodzący na myśl obrazy znane z netflixowskiego serialu Black Mirror.



Rysunek 1: Prezydent Chin - Xi Jinping - przemawiający do narodu

¹New York Times. How China Uses High-Tech Surveillance to Subdue Minorities
<https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html>

Raport dotyczyć będzie dwóch głównych zagadnień:

Łącząc wiedzę odnośnie powstających obecnie alternatywnych metod płatności, cechujących się brakiem kontroli i anonimowością – kryptowalut, a także znając podłoże problemu rosnącej kontroli społecznej na przykładzie Chin i Ekwadoru, postaram się odpowiedzieć na pytanie, czy kryptowaluty są skutecznym narzędziem w walce z brakiem społecznej prywatności. Przykładem, który rozważę będzie kryptowaluta Zcash oraz to, jak ma się ona w stosunku do największej aktualnie kryptowaluty – Bitcoina.

Dokument jest również standardowym raportem na temat kryptowaluty Zcash. Tym razem jednak, w przeciwieństwie do poprzednich raportów, kluczowe wnioski i ocena projektu podzielone zostaną na dwie sekcje – każda z nich dotyczyć będzie jednego z dwóch głównych tematów. Wpierw ocena ogólna i kluczowe wnioski o Zcash, po szczegółowej analizie technologii tej kryptowaluty, zespołu, finansów projektu, rynku, itd. Forma ta sama jak w przypadku reszty moich analiz.

Druga zaś część skupi się na możliwości zastosowaniu Zcash w walce z wyżej opisanym przeze mnie problemem braku prywatności i kontroli obywateli – gdyż Zcash z założenia ma być kryptowalutą oferującą bezpieczeństwo i prywatność finansową. **Moim zdaniem, do właśnie takich sytuacji stworzony został Zcash.**

Serdecznie zapraszam.

stokarz

O autorze

Zajmuję się analizą i badaniem rynku oraz technologii kryptowalut. Raporty mojego autorstwa mają charakter prywatnej opinii, nie stanowią porad inwestycyjnych. **Wykonuje analizy dowolnych kryptowalut na zlecenie.** W celach współpracy proszę o kontakt:

E-mail: stokarzlol@gmail.com

Telegram: @stokarz

Sekcja I – standardowa analiza Zcash (ZEC)

Kluczowe wnioski

- Kryptowaluty nie są prywatne z definicji → w publicznych blockchainach użytkownicy narażeni są na utratę anonimowości, co pokazują liczne badania naukowe.
- Nowe usługi analityczne od Google i firmy takie jak Chainalysis skutecznie deanonimizują kryptowaluty i ich użytkowników.
- Centralne ośrodki zbierające setki tysięcy wchodzących i wychodzących transakcji dokonywanych za pomocą kryptowalut – giełdy – są wrażliwym punktem jeśli chodzi o prywatność.
- **95% adresów w Zcash jest publiczna.**
- Tak wysokie wykorzystanie publicznych adresów ZEC powoduje, że również adresy prywatne – typu „z” – mogą stracić funkcje prywatności.
- Największe giełdy wymiany par walut ZEC/BTC i ZEC/FIAT – np. Gemini i Coinbase, nie akceptują prywatnych adresów ZEC.
- Aby Zcash stał się rzeczywiście prywatny, adresy shielded – prywatne, musiałyby być obowiązkowe.
- Zcash znajduje się w odwiecznym trendzie spadkowym, z powodu niskiej adopcji, dumpowania coinów z Funding Reward oraz braku hodlowania kryptowaluty przez górników.
- Electric Coin Company, firma twórcy Zcash – Zooko Wilcox, organizacja posiadająca całą technologię Zcash – ma zapewnione finansowanie do końca 2020 roku. W ostatnich miesiącach operuje na deficycie budżetowym. Fundusze firmy to, na ten moment, około 5 milionów USD.

- Zcash nie nadaje się do wykorzystania jako rzeczywiście prywatna kryptowaluta, tym samym niemożliwe jest zastosowanie go (w obecnej formie) do walki z zagrożeniem prywatności cywilnej ze strony autorytatywnych rządów, np. w Chinach lub Ekwadorze.
- Drużyna Zcash składa się z światowej klasy deweloperów i naukowców – Zcash posiada zatem doskonałe zaplecze do dalszego rozwoju technologicznego i być może, badacze będą w stanie sprawić, aby Zcash docelowo stał się w pełni prywatny.

Ogólna ocena projektu:

5/10

Sekcja II – Zcash jako narzędzie do przeciwdziałania problemowi kontrolowania społeczeństwa

Ocena projektu

2.5/10

Kryptowaluty - prywatność a anonimowość

W przeciwieństwie do popularnej opinii, używanie kryptowalut nie gwarantuje prywatności². Blockchain będący publicznym rejestrem wszystkich transakcji dokonanych przy pomocy danej kryptowaluty, jest możliwy do przejrzania przez każdego. Jest to niezwykle ważna rzecz – każda osoba, organizacja, rząd na świecie jest w stanie przeglądać transakcje kryptowalutowe. Za przykład weźmy największą i najstarszą z kryptowalut – Bitcoina. Bitcoin jest anonimowy, nie prywatny. Oznacza to, że adresy i transakcje są publiczne, natomiast nie wiadomo zazwyczaj, kto fizycznie jest właścicielem danych monet. Satoshi tworząc Bitcoin³, miał początkowo nadzieję, na uczynienie go prywatnym. Jednak, kiedy już blok Genesis został wykopany, a kryptowaluta zaczęła funkcjonować, okazało się to niemożliwe, jak na technologię tamtych czasów – ponad dziesięć lat temu. Bitcoin pozostał więc anonimowym. Ową anonimowość można jednak złamać. Najczęściej spowodowane jest to ludzką nieświadomością zagrożenia. Wystawiamy swoje adresy na publicznych forach dyskusyjnych, korzystamy z jednego adresu wielokrotnie i nie używamy mikserów zwiększających bezpieczeństwo naszych Bitcoinów (takie narzędzie oferuje Wasabi Wallet albo mobilny portfel Samourai).

Liczne⁴ badania⁵ naukowe dowodzą, że istnieją sposoby, takie jak analiza klastrowa⁶, czy śledzenie wejść i wyjść nawet prywatnych kryptowalut, przepływających przez adresy giełdowe⁷, które niszczą prywatność, a dokonujący takiej analizy jest się w stanie powiązać określone adresy z fizycznymi osobami. Z wysoką pewnością można stwierdzić, że skutecznymi metodami łamania prywatności kryptowalut dysponują już od dawna liczne agencje wywiadowcze i ośrodki naukowe na całym świecie. Dlatego tak ważne jest, abyśmy używali każdego z adresów tylko i wyłącznie raz. Taka praktyka powoduje, że zachowujemy anonimowość i jesteśmy praktycznie nie do wyśledzenia. Nie przesadzę, jeżeli powiem, że trwa wojna – między tymi, którzy chcą zapewnić nam prywatność, a osobami próbującymi tą prywatność złamać. Od stuleci taka sytuacja miała miejsce w kryptografii. Szczegółowa analiza rejestru transakcji kryptowalut staje się ostatnio coraz łatwiejsza i dostępna dla każdego w zaciśnięciu jego własnego domu. Znany wszystkim gigant technologiczny - Google⁸, mistrz jeżeli

² Coin Center. How anonymous is Bitcoin <https://coincenter.org/entry/how-anonymous-is-bitcoin>

³ Bitcoin: A Peer-to-Peer Electronic Cash System <https://bitcoin.org/bitcoin.pdf>

⁴ An Analysis of Anonymity in the Bitcoin System <https://arxiv.org/abs/1107.4524>

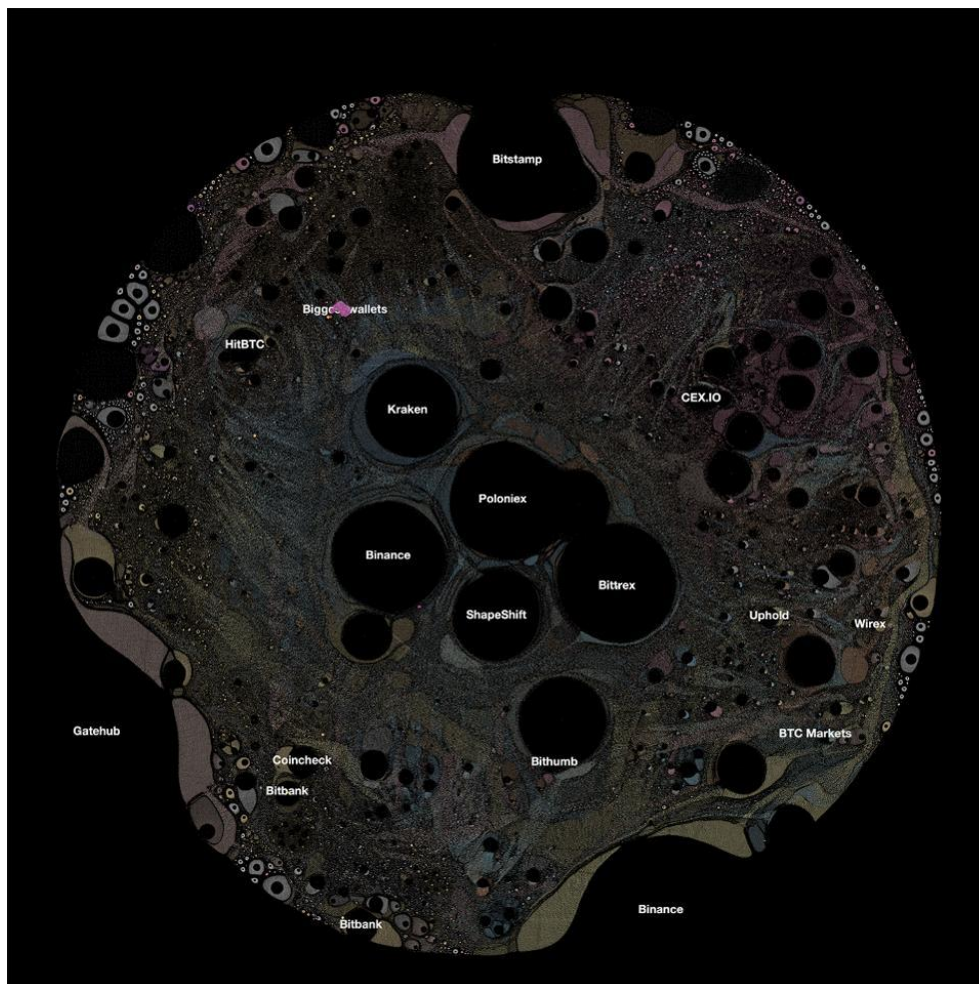
⁵ Privacy risks of web payments via cryptocurrencies <https://arxiv.org/abs/1708.04748>

⁶ Automatic Bitcoin Address Clustering https://bitfury.com/content/downloads/clustering_whitepaper.pdf

⁷ Tracing Transactions Across Cryptocurrency Ledgers <https://arxiv.org/pdf/1810.12786.pdf>

⁸ Navigating Bitcoin, Ethereum, XRP: How Google Is Quietly Making Blockchains Searchable <https://www.forbes.com/sites/michaeldelcastillo/2019/02/04/navigating-bitcoin-ethereum-xrp-how-google-is-quietly-making-blockchains-searchable/#1d4fd2cc4248>

chodzi o nawigację w sieci – od miesiący prowadził prace nad narzędziami do analizy blockchaina popularnych kryptowalut. Usługa jest już dostępna w Google Cloud⁹. Nawet wykorzystanie sieci TOR może nie być rozwiązaniem problemu braku prywatności Bitcoina¹⁰.



Rysunek 2: Giełdy, dla analityków blockchaina, są jak mocno świecące latarnie morskie, do których płyną wszyscy żeglarze.

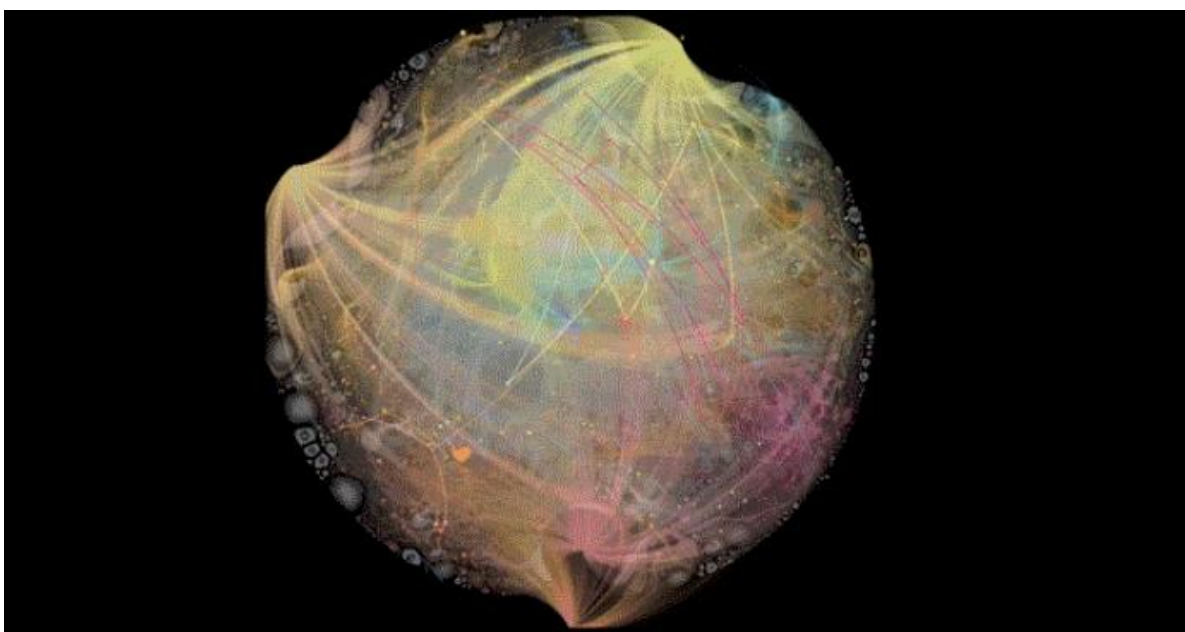
Wszystko to pokazuje, że jeżeli adres zostanie przypisany, poprzez naszą nieuwagę lub zwykły błąd ludzki, do fizycznej osoby, cała historia naszych płatności przy pomocy kryptowalut może zostać odkryta. Śledzenie transakcji kryptowalutowych staje się coraz łatwiejsze, a liczne narzędzia i firmy oferują pomoc w przeprowadzeniu analizy blockchaina.

⁹ Google Cloud: Introducing six new cryptocurrencies in BigQuery Public Datasets <https://cloud.google.com/blog/products/data-analytics/introducing-six-new-cryptocurrencies-in-bigquery-public-datasets-and-how-to-analyze-them>

¹⁰ Bitcoin over Tor isn't a good idea <https://arxiv.org/pdf/1410.6079.pdf>

Jeden z praktycznych sposobów przypisywania transakcji kryptowalutowych do realnych osób został opisany w badaniu naukowym przeprowadzonym przez naukowców z Uniwersytetu Kalifornijskiego¹¹:

Aby wykonać to zadanie, opracowaliśmy nową heurystykę klastrowania opartą na adresach zmian, umożliwiającą nam grupowanie adresów należących do tego samego użytkownika. Następnie, wykorzystując niewielką liczbę transakcji oznaczonych przez nasze własne interakcje empiryczne z różnymi usługami, identyfikujemy główne instytucje i interakcje między nimi. Nawet nasz stosunkowo niewielki eksperyment pokazuje, że takie podejście może rzucić znaczne światło na strukturę gospodarki Bitcoina.



Rysunek 3: Google - wizualizacja cyfrowej księgi rozrachunkowej Ripple (XRP)

Rzeczywiste zachowanie prywatności w czasie korzystania z kryptowalut jest więc trudnym zadaniem. Miejmy nadzieję, że usprawnienia prywatności takie jak sygnatury Schnorra zostaną w niedalekiej przyszłości zaimplementowane do głównego protokołu Bitcoina. Jak dowodzi Bitmex Research¹², długofalowo zwiększyłoby to znacząco prywatność BTC, utrudniając powiązywanie transakcji i adresów.

Na razie jednak zdrowy rozsądek pozostaje najlepszym narzędziem w walce o prywatność w czasie używania kryptowalut. Co jednak, gdybyśmy chcieli pójść o krok dalej? Dziś istnieją już

¹¹ A Fistful of Bitcoins: Characterizing Payments Among Men with No Names
<https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>

¹² The Schnorr Signature & Taproot Softfork Proposal
<https://blog.bitmex.com/the-schnorr-signature-taproot-softfork-proposal/>

kryptowaluty skupiające się na prywatności użytkownika. Są to między innymi: Monero (XMR), Dash (DASH) i Zcash (ZEC). Dalsza część raportu skupi się na tym ostatnim.

Zcash – prywatna kryptowaluta

Wprowadzenie

Zcash (ZEC) jest kryptowalutą przeznaczoną do prywatnych płatności cyfrowych. Wykorzystuje najnowocześniejszą technologię kryptograficzną w celu zapewnienia zaawansowanych funkcji prywatności swoim użytkownikom. Choć technologia jest naprawdę imponująca, niskie wskaźniki przyjmowania transakcji prywatnych pokazują, że moneta jest daleko w tyle pod względem wykorzystania jej jako rzeczywiście prywatnej.

Ponadto Zcash stoi w obliczu szeregu zagrożeń związanych z rosnącą konkurencją, regulacjami rządowymi, potencjalnymi przyszłymi problemami z finansowaniem i zarządzaniem firmą Electric Coin Company, zajmującej się Zcash, które mogą negatywnie wpłynąć na jego udział w rynku i bazę użytkowników.

Kontynuując ulepszenia technologiczne, zespół musi skupić się na wprowadzeniu obowiązkowej prywatności poprzez stosowanie adresów prywatnych – typu „z”. Moneta musi spełniać swoje zadanie. W przeciwnym razie może nigdy nie dojść do powszechnej adopcji i Zcash pozostanie w stanie rywalizacji z wieloma nieprywatnymi rywalami, którzy są znacznie bardziej zaawansowani, chociażby z Bitcoinem. Szczególnie jeżeli zostaną w nim zaimplementowane funkcje zwiększające prywatność, jak np. sygnatury Schnorra.

Zcash jest oparty na kryptografii funkcji eliptycznej konstruktu (po softforku Sapling) BLS12 – 318 i wykorzystuje w swoim protokole POW (Proof of Work – dowód pracy) algorytm Equihash. Zcash nie jest domyślnie prywatny, a jego adresy dzielą się na „t” oraz „z” – transparentne i prywatne. Dzienna inflacja podaży Zcash wynosi 0.151%, także jest znacznie większa od inflacji rywalów rynkowych, jak Monero czy Dash.

Zcash wykorzystuje technologię Zero Proof Knowledge (w Zcash: zk-SNARKs) do ukrywania historii transakcji i adresów użytkowników. Zcash powstał z protokołu Zerocoina, opracowanego w 2013 roku.

W maju 2018 roku udało się wprowadzić parametry Equihash do układów ASICs¹³. Spowodowało to spadek w aktywnych adresach ze 119 tys. do 17 tys.

Ważne statystyki Zcash:

Maksymalna ilość monet: 21,000,000 ZEC

Wydobytych monet: 1,672,744 ZEC

Pierwszy blok: 2016-10-28

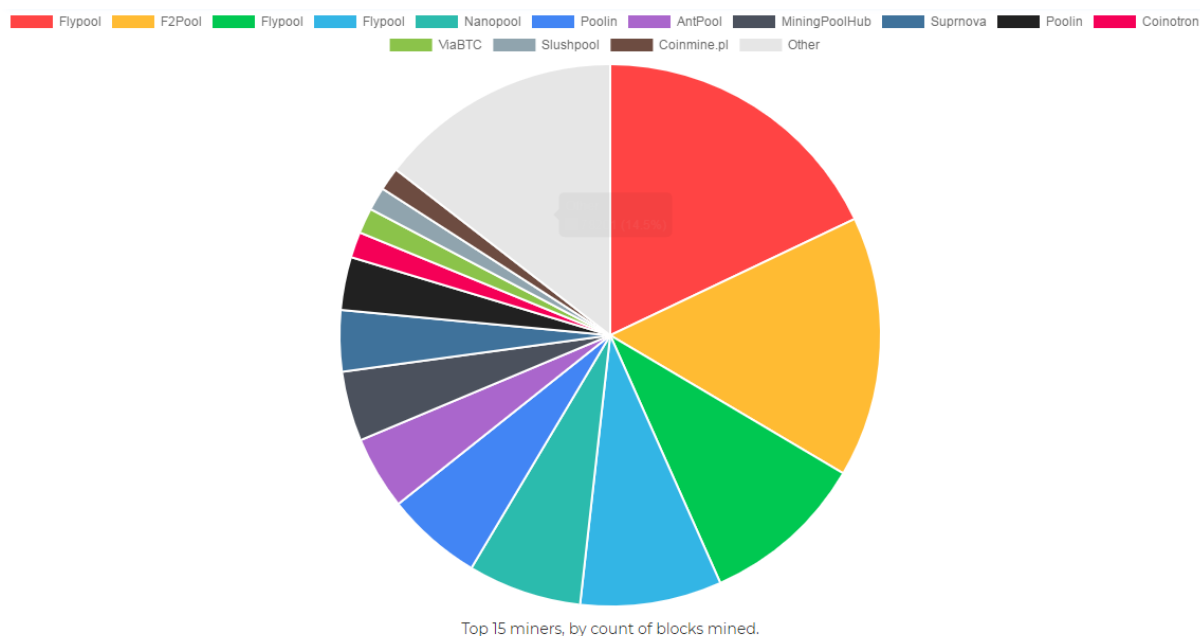
Liczba bloków: 143819

Średni czas pomiędzy blokami: 2m 30s

Nagroda w bloku: 12,5 ZEC

Algorytm: Equihash

Rysunek 4: Źródło - Bithub.pl



Rysunek 5: Historyczne wydobywanie ZEC od pierwszego bloku do teraz – Flypool jest największą kopalnią

¹³ Zcash – ASICs <https://z.cash/blog/zcash-company-statement-on-asics/>

Nad rozwojem Zcash sprawują pieczę dwa organy: Electric Coin Company, założona przez Zooko Wilcoxa, twórcę Zcash (ZEC), i posiadająca wszelkie prawa do technologii Zcash, oraz Zcash Foundation, założona niedawno fundacja non-profit, która w przyszłości ma skupić się na rozwoju Zcash. Obie z tych instytucji finansowane są za pomocą Funding Reward. Polega to na tym, iż 20% z wszystkich nagród z bloków wykopanych przez górników przeznaczane jest dla ECC i Zcash Foundation, a także założycieli i wczesnych partnerów. Funding Reward zostanie szczegółowo omówiona w dalszej części raportu.

Czym jest Zcash

W dzisiejszym świecie jesteśmy w stanie dokonywać płatności poprzez różnego rodzaju „media”: karty kredytowe, gotówkę, czy właśnie kryptowaluty. Jak w tym spektrum wypada Zcash?

Bitcoin vs Zcash vs Credit card vs Cash			
Bitcoin	Zcash	Credit card	Cash
Efficient	Efficient	Efficient	Inefficient
Attack- and censorship-resistant	Attack- and censorship-resistant	Open to attack or censorship	Not secure
Auditable	Auditable with user permission	Auditable with user permission	Not auditable
Not private	Private	Limited privacy	Private

Rysunek 6: Zcash, a gotówka i karty kredytowe

Zcash, będąc kryptowalutą opartą o globalny i publiczny rejestr transakcji – blockchain, jest wydajny, szybki w przesyle i anonimowy. Jak wykażę w dalszej części raportu, wysokie zastosowanie publicznych adresów w ZEC sprawia, że nie jest on w rzeczywistości prywatny.

Chciałbym również całkowicie zaprzeczyć wnioskowi płynącemu z raportu Grayscale¹⁴, jakoby Zcash był w stanie stać się medium, w którym lokowany będzie międzynarodowy kapitał pochodzący z rajów podatkowych – tym samym cena Zcash wzrośnie do niebotycznych rozmiarów (Grayscale prognozuje 60 tys. USD za jedną monetę ZEC). Dokonywanie transakcji za pomocą ZEC nie jest, na tą chwilę, prywatne. Dodatkowo, nie istnieją „bramki” pozwalające

¹⁴ Grayscale. Zcash Investment Thesis <https://grayscale.co/wp-content/uploads/2018/01/Grayscale-Zcash-Investment-Thesis-protected.pdf>

nam na upłynnienie naszych ZEC i sprzedaż monet za tradycyjne waluty FIAT, gdyż giełdy nie akceptują prywatnych adresów Zcash.

Jeżeli jednak Zcash, poprzez rozwój technologiczny, stałby się w całości prywatny, potencjalne tradycyjne drogi przesyłania kapitału, z którymi może konkurować to:

Project Name	Ticker	Competing Product	Key Features	Market Cap
Western Union	WU	Money transfers	* 200 countries * 550,000 agent locations * 150,000 ATMs, Kiosks	\$8.218 billion
Mastercard	MA	Payment systems	* debit/credit cards * more than 1700 tps * merchant, transaction, and processing infrastructure	\$12.469 billion
PayPal	PYPL	Online payments system	* 202 countries * 244 million active accounts * 25 currencies worldwide	\$100,761 bln.

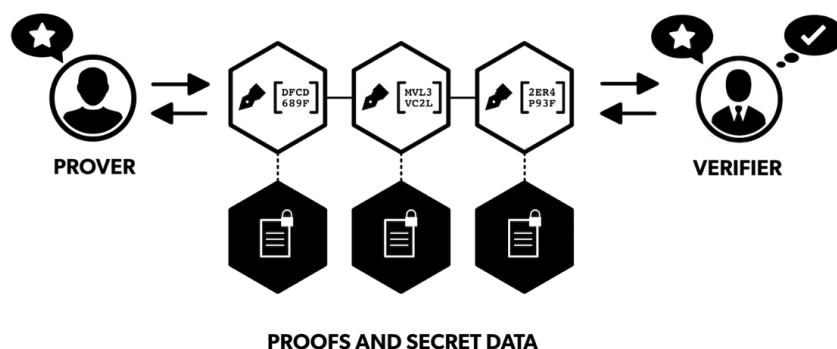
Rysunek 7: WU, MC i PAYPAL

W dalszej części raportu skupimy się na określeniu realnego zastosowania Zcash, aktywności sieci, ilości użytkowników oraz odpowiemy sobie na pytanie – czy transakcje dokonywane za pomocą Zcash są rzeczywiście prywatne? Na tyle, aby móc zastosować je do walki z autorytatywnymi organami rządowymi (ten problem przedstawiłem na początku raportu).

Część II

Analiza kryptowaluty Zcash

Zcash swoje działanie opiera na niezwyklej matematycznym przełomie dokonany w 1989¹⁵ roku – wynalezieniu Zero Knowledge Proof. Jak znaczące było to odkrycie potwierdza otrzymanie, przez grupę zaangażowanych w badania naukowców, nagrody Godla – nazywanego matematycznym Noblem.



Rysunek 8: Uproszczony schemat funkcjonowania ZeroNP

Zero Knowledge Proof (dalej ZKP) pozwala udowodnić, że wiesz coś, bez przekazywania i odkrywania tej informacji. Jeżeli zastanowimy się nad tym głębiej, jest to doprawdy niesamowite odkrycie. Jesteśmy w stanie fizycznie potwierdzić, że posiadamy daną informację bez ujawniania jej. Ilość zastosowań takiego systemu, jaka przychodzi do głowy, jest zatrważająca.

ZKP mogłoby np. zostać wprowadzone w tradycyjny system kredytowy – osoba starająca się o pożyczkę, nie musiałaby ujawniać konkretnej sumy swoich dochodów. Zamiast tego bank

¹⁵ Wikipedia. Zero Knowledge Proof. https://en.wikipedia.org/wiki/Zero-knowledge_proof

sprawdzałby, czy dochody wnioskującego znajdują się w pewnym przedziale wymaganym do udzielenia pożyczki. Osoba zainteresowana, przy pomocy ZKP, utworzyłaby wtedy kryptograficznie bezpieczny i pewny dowód, że jej dochody znajdują się w wymaganym przedziale (lub nie) i finalnie bank byłby w stanie udzielić kredytu. Dlaczego ma to znaczenie? Gdyż coraz silniejsze regulacje w USA i Europie (z ramienia Unii Europejskiej) odnośnie przechowywanych danych klientów powodują, że w przyszłości, bardziej opłacalne dla banku może być zbieranie jak najmniejszej ilości wrażliwych danych – w tym o dokładnych finansach klientów – w celu uniknięcia regulacji prawnych. Dotyczy to szczególnie instytucji, które rozwijają technologię z dziedziny FinTech. Jak dotąd, firmy gromadziły tyle danych, ile było to możliwe. Niedługo, może się okazać, że model w którym prywatna firma gromadzi jak najmniej wrażliwych danych, w celu uniknięcia niepotrzebnych regulacji, jest bardziej opłacalny ekonomicznie.

Twórca Zcash, Zooko Wilcox, już w latach 90, tuż po wynalezieniu ZNP, pracował nad zastosowaniem ich w cyfrowym systemie monetarnym. Za każdym razem, pewna bariera okazywała się nie do pokonania – decentralizacja. Nie istniał sposób, jak stworzyć cyfrową walutę, która nie podlegałaby kontroli centralnego organu, tym samym nie byłaby narażona na potencjalne ataki, chociażby ze strony regulacji rządowych. Dopiero Satoshi Nakamoto zaprezentował światu, jak stworzyć prawdziwy pieniądz cyfrowy, który nie byłby pod niczyją kontrolą. Wilcox, mając w końcu klucz do stworzenia prywatnego cyfrowego pieniądza i zastosowania w nim ZNP, wiedział jaką drogą należy pójść.

W Zcash ma to konkretne zastosowanie – jesteśmy w stanie płacić kryptowalutą bez ujawniania ile jej rzeczywiście posiadamy na naszym adresie. Nie ujawniamy również swojej historii transakcji. Zatem płatności odbywają się całkowicie prywatnie i anonimowo. Tak przynajmniej wygląda to w teorii. Niestety, byłoby chyba zbyt pięknie, gdyby rzeczywistość za każdym razem odwzorowywała teorię. Wrócimy jeszcze do tego argumentu. Zero Knowledge Proof z jakich korzysta Zcash, noszą nazwę zk-SNARKs¹⁶.

Definicja zk-SNARKs: Dowód, że wykonałeś obliczenia na niektórych wejściach, bez ujawniania danych wejściowych.

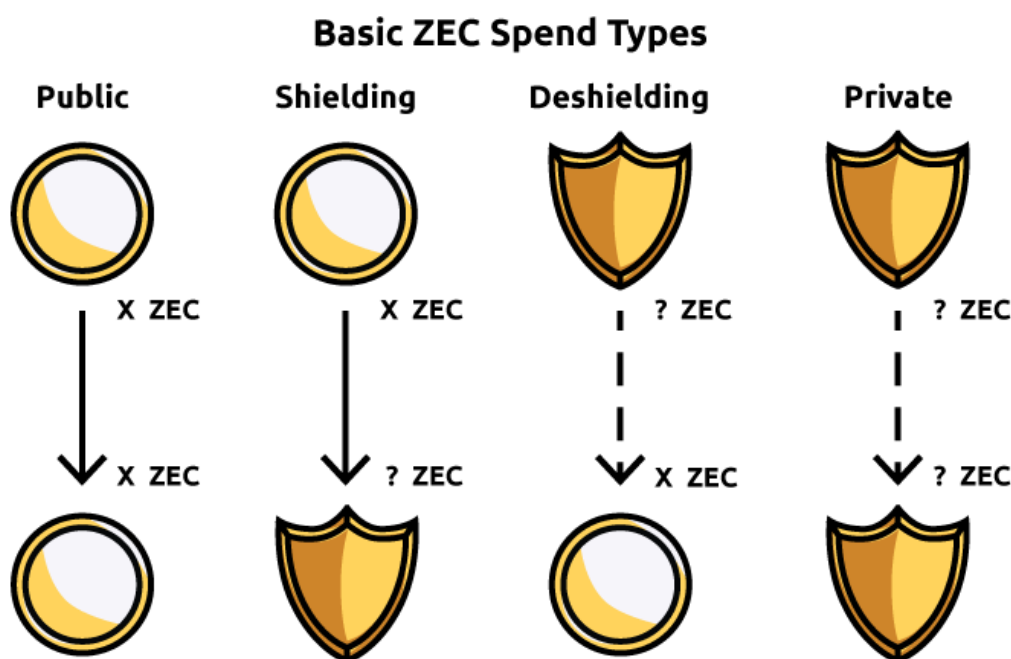
¹⁶ zk-SNARKs Zcash <https://z.cash/technology/zksnarks/>

Anatomia transakcji Zcash

Zcash posiada dwa rodzaje adresów. Według słów założycieli, wierzących w wolność wyboru w sprawach finansowych, człowiek korzystający z kryptowalut powinien mieć wybór – czy chce, aby historia jego transakcji była publicznie dostępna dla wszystkich (np. ponieważ prowadzi fundację i chciałby, aby jej finanse były transparentne), czy też ceni sobie prywatność i zamierza ukryć ilość posiadanych przez siebie jednostek kryptowaluty.

Dwa rodzaje adresów w kryptowalucie Zcash¹⁷:

- Adresy „t” – transparentne, z publicznie widoczną historią transakcji.
- Adresy „z” – prywatne, tzw. z ang. shielded (zabezpieczone). Historia transakcji nie jest widoczna publicznie.



Rysunek 9: Rodzaje transakcji w Zcash

W kryptowalucie Zcash możemy wyróżnić cztery typy transakcji. Pierwsza z nich to transakcja typu „t” → „t”. Ma ona miejsce, kiedy przesłanie Zcash dokonuje się między dwoma publicznymi adresami. W takim wypadku monety nie są prywatne, aczkolwiek zachowują

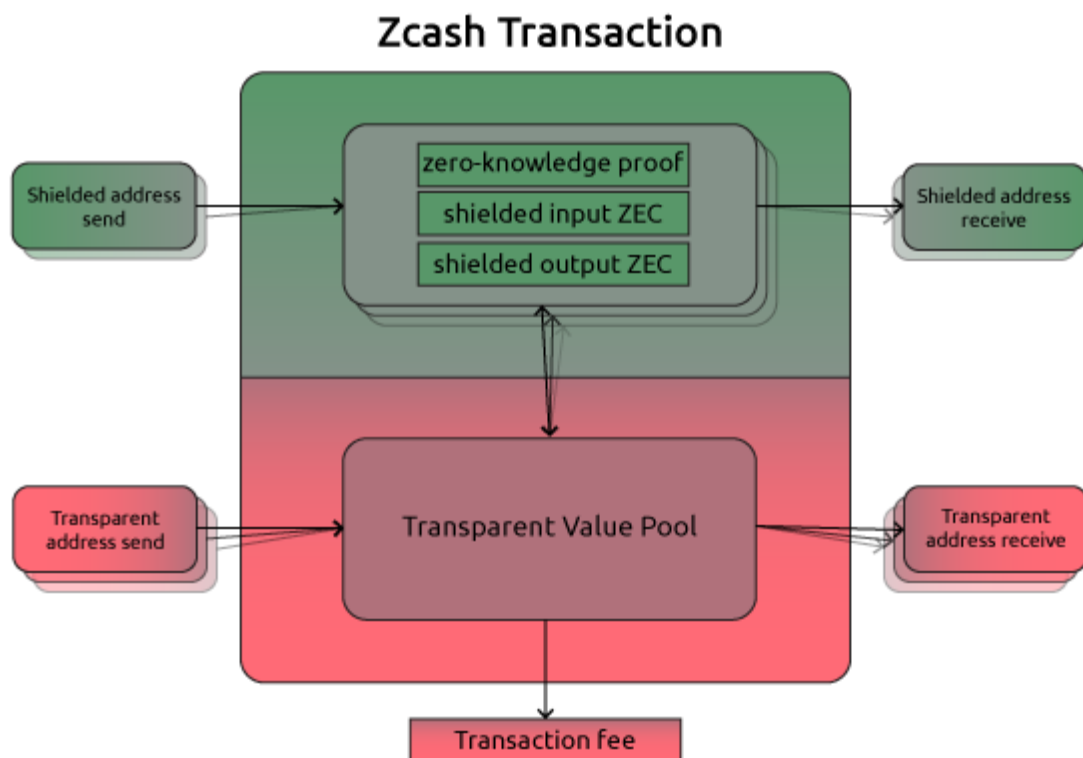
¹⁷ Transaction anatomy of Zcash. <https://z.cash/blog/anatomy-of-zcash>

swoją anonimowość. Jest to zatem taka sama sytuacja, jak w przypadku transakcji dokonywanych przy użyciu Bitcoinie.

Druga kategoria to transakcje typu „t” → „z”, nazywana również shielding. Jest to transakcja z adresu publicznego do adresu prywatnego.

Następnie mamy możliwość dokonania tzw. deshielding, czyli przesłania środków z prywatnego adresu na adres publiczny. Jest to trzecia kategoria transakcji, oznaczana symbolicznie jako „z” → „t”.

Ostatni z rodzajów transakcji „z” → „z” jest jedynym, który zapewnia nam prywatność. Jest to transakcja dokonana pomiędzy dwoma prywatnymi adresami, bez ujawniania jakiegokolwiek historii transakcji. Chcąc korzystać z funkcjonalności prywatności oferowanej przez Zcash, jest to jedyny rodzaj transakcji, którym powinniśmy się posługiwać. Tylko taka transakcja zapewnia rzeczywistą prywatność.



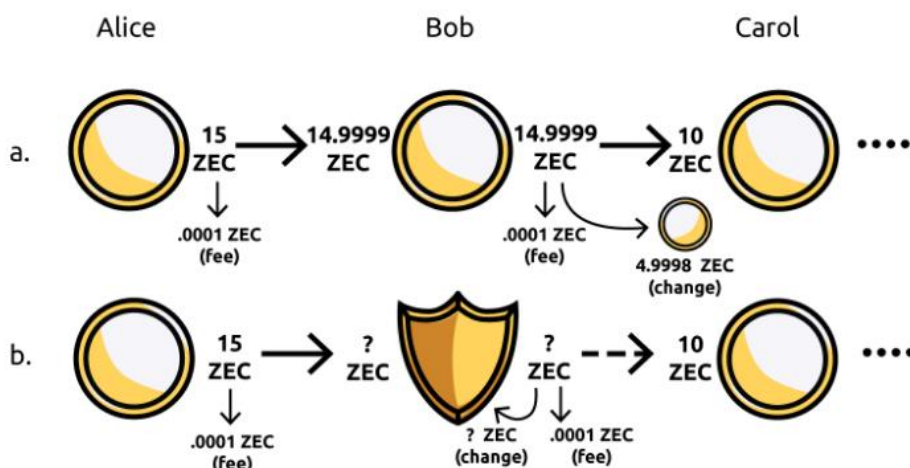
Rysunek 10: Zastosowanie ZKP do konstrukcji transakcji Zcash

Zagrożenia prywatności dla transakcji przy pomocy Zcash

Wiedząc już jak dokładnie wyglądają transakcje, zastanówmy się, co może zagrozić bezpieczeństwu i realnej prywatności kryptowaluty Zcash.

Zcash opiera swoją sieć na kryptografii funkcji eliptycznej, tak samo jak Bitcoin. Kryptografia funkcji eliptycznej nie jest obecnie możliwa do złamania. Dodatkowo, w niedawnym softforku Sapling¹⁸ Zcash, dokonano usprawnienia tego aspektu protokołu, tworząc konstrukt funkcji eliptycznej typu Barreto-Naehrig, zastępując BLS12 – 381. Cytując:

Sapling pozwolił również na to, aby sprzęt, który konstruuje dowód zk-SNARK, był niezależny od sprzętu podpisującego transakcję, zapewniając użytkownikom większą elastyczność w wysyłaniu transakcji. Ulepszone klucze umożliwiają również właścicielom adresów na urządzeniach typu hardware, wyświetlanie szczegółów transakcji przychodzących i wychodzących bez narażania ich klucza prywatnego. Wreszcie Sapling zintegrował również krzywą eliptyczną BLS12-381, która poprawia istniejącą konstrukcję krzywej eliptycznej Barreto-Naehriga. Nowa implementacja krzywej eliptycznej jest bardziej wydajna niż poprzednia, poprawiając wydajność i czas weryfikacji dowodów zk-SNARK.

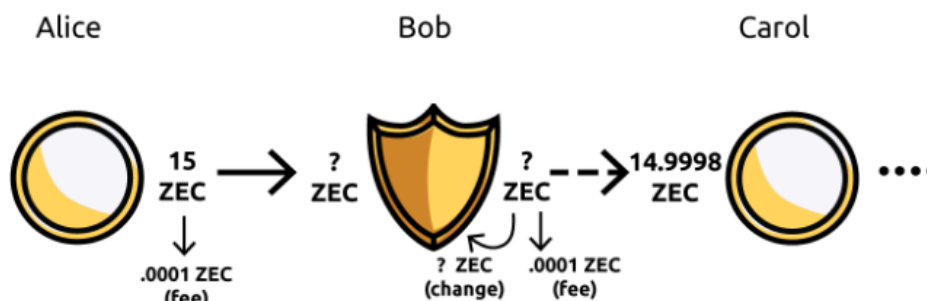


Rysunek 11: Transakcja publiczna - a. Transakcja z wykorzystaniem prywatnego adresu -b.

Kryptografia, z której korzysta Zcash jest bezpieczna. Utrata prywatności może jednak zajść na poziomie transakcji. Kiedy kryptowaluta przechodzi z adresów publiczny („t”) do prywatnych („z”) i z powrotem na publiczne („t”) adresy, mogą one utracić część anonimowości, jaką

¹⁸ Sapling Softfork Zcash <https://blockonomi.com/zcash-sapling-upgrade/>

posiadały. Mówimy zatem o prostym schemacie transakcji „t” → „z” → „t”. Adres publiczny, adres prywatny i znów na adres publiczny.



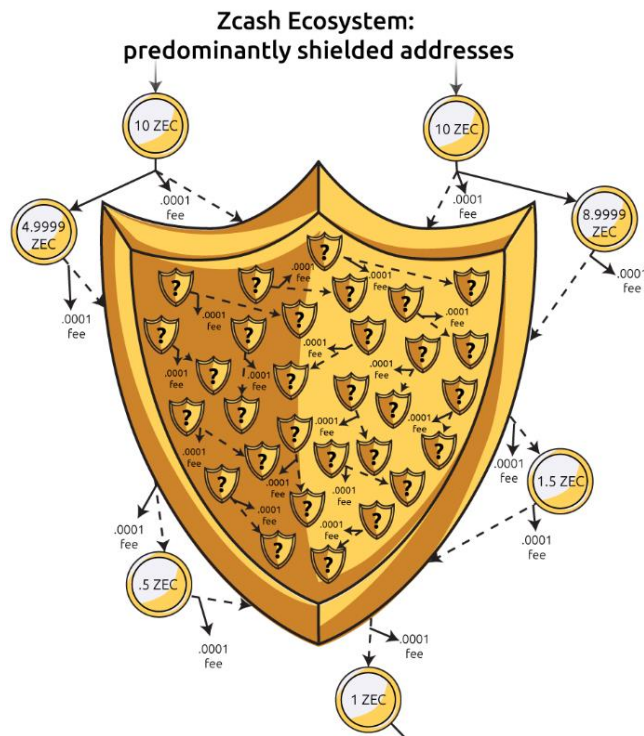
Rysunek 12: Transakcja "t" - "z" - "t"

Takie zachowanie, pomimo zastosowania prywatnego adresu w naszym łańcuchu transakcji, powoduje, że postronny obserwator przeprowadzający analizę blockchajna, wie doskonale ile ZEC znajdowało się na prywatnym adresie – w powyższym wypadku jest to 5 ZEC. Deweloperzy Zcash są w pełni świadomi zagrożenia. Zaadresowali je nawet w jednej ze swoich publikacji na blogu¹⁹:

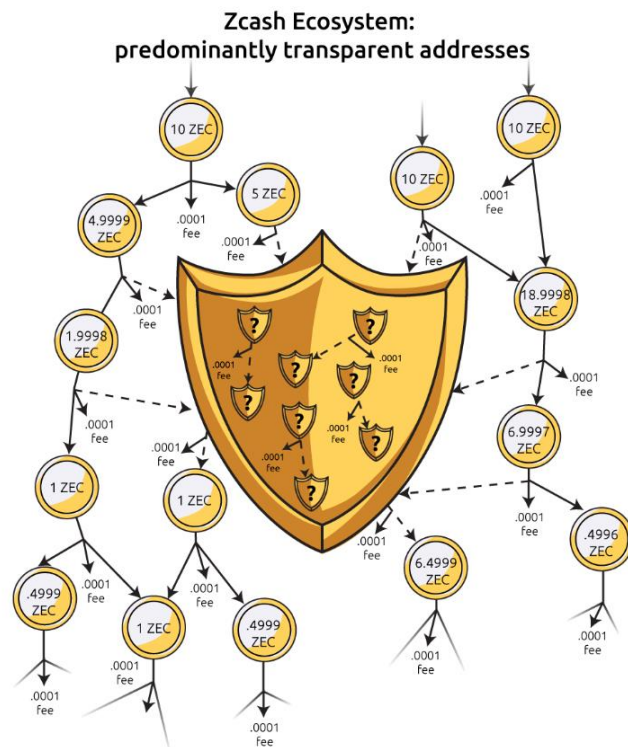
Aby wyjaśnić dlaczego jest to niebezpieczne, najpierw zaznaczmy właściwość transakcji, które zawierają oba typy adresów: gdy publiczne adresy uprywatniają informacje o swoich ZEC (t → z) lub gdy prywatne adresy odsyłają ZEC (z → t), wartości wysyłane do lub odbierane z publicznych adresów są transparentne, nawet jeśli te wartości są maskowane w prywatnej części adresu transakcji. Możemy zaobserwować tę właściwość w serii transakcji powyżej, gdzie Bob używa prywatnego adresu, ale publiczne adresy używane przez Alice i Carol nadal ujawniają przesłaną i odebraną wartość.

Zatem w celu zachowania anonimowości, dokonywane przez nas transakcje kryptowalutą ZEC powinny zawsze przechodzić z prywatnego adresu na inny prywatny adres. Ważne również jest, aby ogólna ilość wszystkich transakcji w obrębie blockchajna Zcash była prywatna w min. 90%. W przeciwnym razie, możliwe jest utworzenie połączeń między adresami publicznymi i prywatnymi, co finalnie prowadzi do zdobycia wiedzy na temat tego, ile jednostek kryptowaluty przechowują lub przechowywały poszczególne adresy prywatne. Im mniejsza ilość adresów prywatnych w sieci i im większa ilość publicznych, tym cechy prywatności Zcash są słabsze. Obrazują to dwa schematy:

¹⁹ Zcash transaction linkability <https://z.cash/blog/transaction-linkability/>



Rysunek 13: Przeważająca ilość adresów ZEC jest prywatna - powiązanie ze sobą transakcji jest niezwykle trudne



Rysunek 14: Publiczne adresy stanowią przeważającą większość - badanie połączeń między prywatnymi, a publicznymi adresami jest stosunkowo proste

Jeżeli Zcash miałby być prywatny, analiza blockchaina powinna wykazać, że posiadanie prywatnych adresów jest przez użytkowników faworyzowane, a i łączna ilość wynosi ponad 90%. Spójrzmy więc co mówią nam dane.

Rzeczywista prywatność kryptowaluty Zcash

Kiedy przygotowywałem się do napisania tego raportu, początkowo takie wolnościowe podejście przypadło mi do gustu. Zdaje się być logiczne i posiadające sens. Użytkownik ma wybór – transparentność czy całkowita prywatność. Bardzo szybko jednak byłem zmuszony odstawić na bok swoje przekonania o użyteczności i słuszności tego rozwiązania w Zcash.

Analiza blockchaina²⁰ wykazała, że 95% wszystkich adresów Zcash jest typu „t”. Zatem są publiczne, tak jak w przypadku Bitcoina.



Rysunek 15: Źródło - blockchain Zcash.

W pierwszej kolumnie widzimy ilość ZEC znajdującą się na publicznych adresach. Kolumny numer dwa i trzy obrazuje łączny procent monet ZEC posiadających cechę prywatności. Wyniki są z lekka szokujące, gdyż oznaczają, że w praktyce Zcash nie jest prywatną kryptowalutą, a prawie wszystkie ZEC przebywają na publicznych adresach. Jedyne pytanie, które nasuwa się w takim momencie – dlaczego dziesiątki artykułów przeczytanych przeze mnie jako wprowadzenie do Zcash zgodnie twierdzi, że jest on w pełni prywatny i bezpieczny? Odpowiedź jest nieco szokująca – na chwilę obecną, pod względem prywatności ZEC nie różni się niczym od Bitcoina.

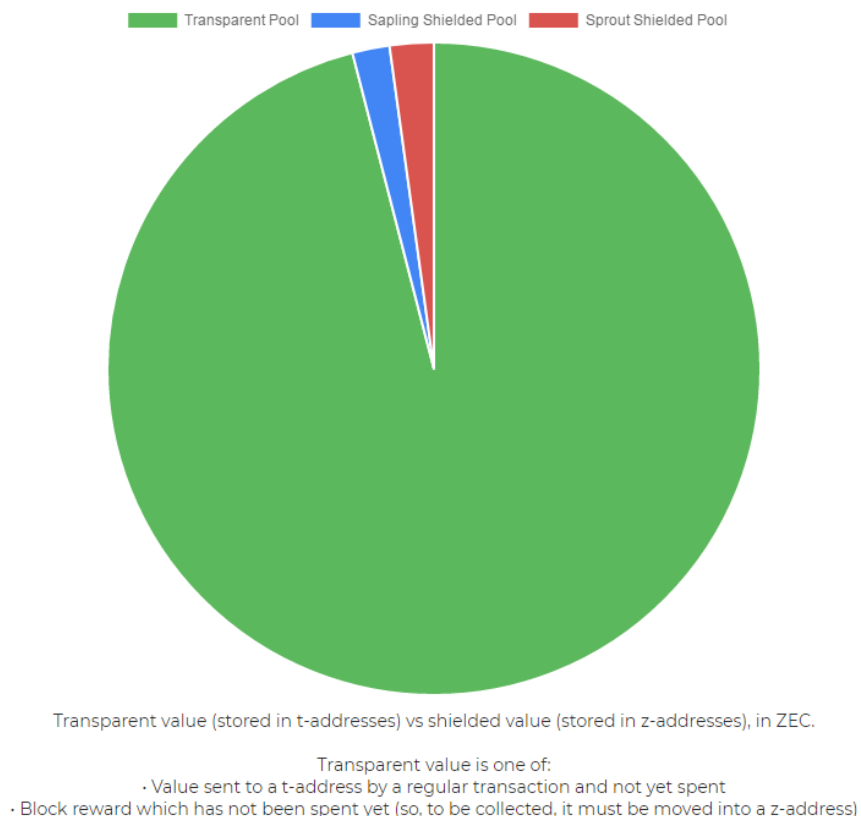
Wykorzystanie prywatnych adresów Zcash powinno być obowiązkowe. Tak wielka ilość adresów publicznych sprawia, że nawet prywatne adresy są zagrożone, gdyż możliwe jest utworzenie mapy powiązań i w konsekwencji wysoce dokładne określenie historii transakcji adresów prywatnych. Dowodzi tego kolejna statystyka:

²⁰ Zbiory danych blockchaina kryptowaluty Zcash <https://explorer.zcha.in/statistics/network>

Timerange	Transparent Tx	Shielded Tx	Fully Shielded Tx	Transparent Value Transacted	Shielded Value Transacted (lower bound)
Past Hour	148	22	6	117019 ZEC	497 ZEC
Past Day	3592	368	55	1378173 ZEC	6673 ZEC
Past Week	25460	2610	366	9713375 ZEC	95699 ZEC
Past Month	120254	10934	1183	59172428 ZEC	319729 ZEC

Rysunek 16: Statystyka transakcji w sieci ZEC

Jak mówiłem wyżej, tylko transakcje między dwoma prywatnymi portfelami zapewniają prywatność (która może być naruszona, jeżeli dane monety kiedykolwiek opuszczą prywatne adresy). W ciągu 30 dni, transakcje typu „z” → „z” stanowiły raptem mniej niż 1% wszystkich transakcji w sieci. Ilość transakcji z prywatnego adresu na publiczny lub z publicznego na prywatny wynosiła 10 934 transakcji, czyli ok. 8%. **Transakcje między publicznymi adresami odpowiadały za prawie 91% wszystkich transakcji**, skutecznie pozbawiając tym samym całą sieć prywatności.



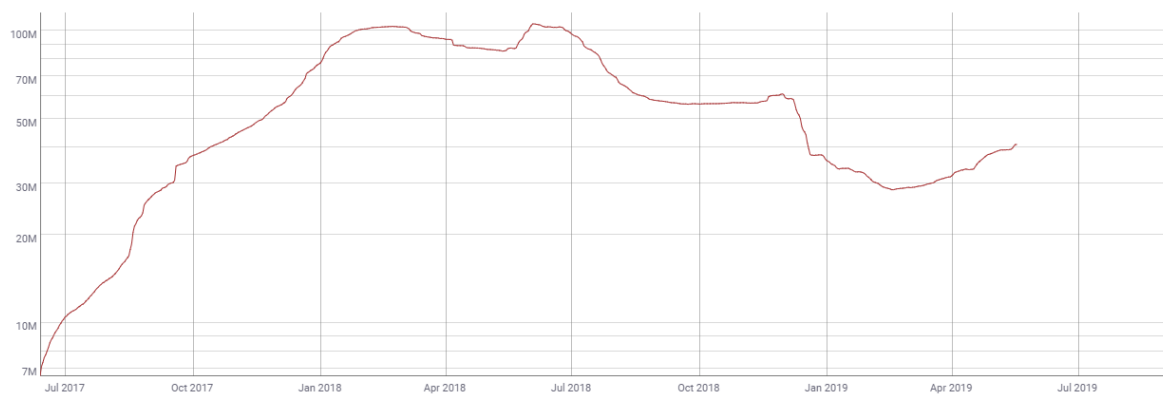
Rysunek 17: Rozłożenie ogólnej wartości kryptowaluty ZEC na poszczególne rodzaje adresów

Pomimo wprowadzenia usprawnień w zakresie tworzenia prywatnych transakcji, dane historyczne obrazują, że kiedyś użytkownicy tworzyli więcej prywatnych transakcji²¹. W 2017 roku, 19.6% transakcji zawierało w sobie adresy typu „z”, z czego 98% z tych transakcji było w postaci „t-z” lub „z-t”. Transakcje typu „z-z” to rzadkość. Jeżeli dodamy do tego statystyki pokazujące, jak zmienia się liczba aktywnych adresów Zcash oraz ogólna liczba transakcji w blockchainie, spadek w prywatnych transakcjach jest jeszcze wyższy.



Rysunek 18: Liczba aktywnych adresów Zcash - źródło: Coin Metrics

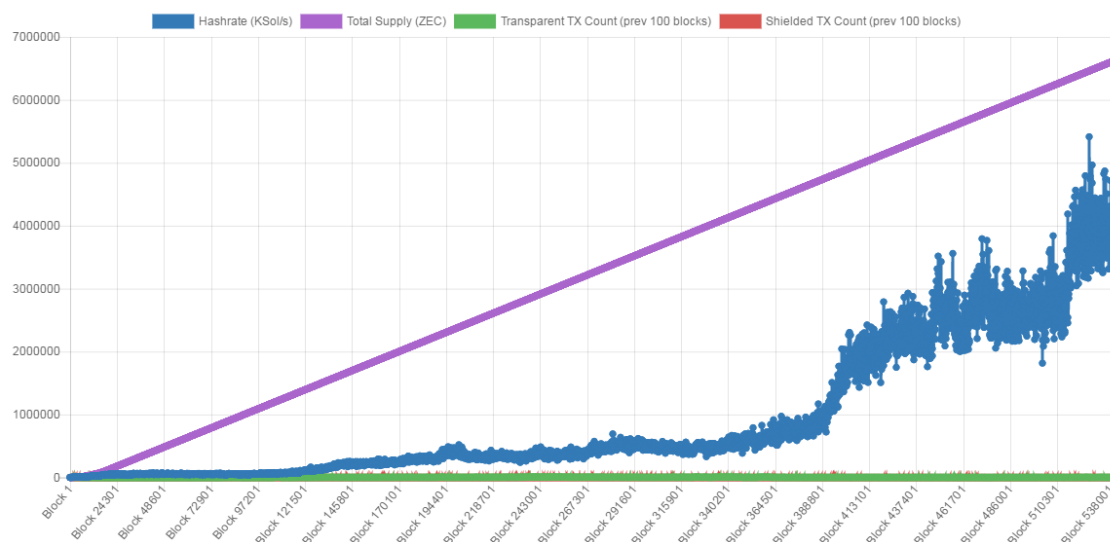
Spadek zanotował również całociowy średni wolumen transakcyjny ZEC:



Rysunek 19: Średni wolumen transakcji ZEC (w USD)

Ostatni z wykresów pokazuje, jak od początku zmieniła się ogólna podaż Zcash i hashrate oraz, jakie przełożenie ma to na typy transakcji ZEC.

²¹ On Zcash transaction linkability. <http://jeffq.com/blog/on-the-linkability-of-zcash-transactions/>



Rysunek 20: Ilość prywatnych transakcji w ZEC maleje (czerwone kreski na dole wykresu). Niebieskim oznaczony jest hashrate, na zielono publiczne transakcje, a fioletowa linia to podaż kryptowaluty.

Wniosek: Prywatność nie powinna być opcją - wyborem. Powinna być obowiązkowa. Uproszczenie systemu Zcash i wyeliminowanie publicznych adresów sprawiłoby, że kryptowaluta stałaby się rzeczywiście prywatna. Dlaczego więc tak się nie dzieje?

Dwa główne powody:

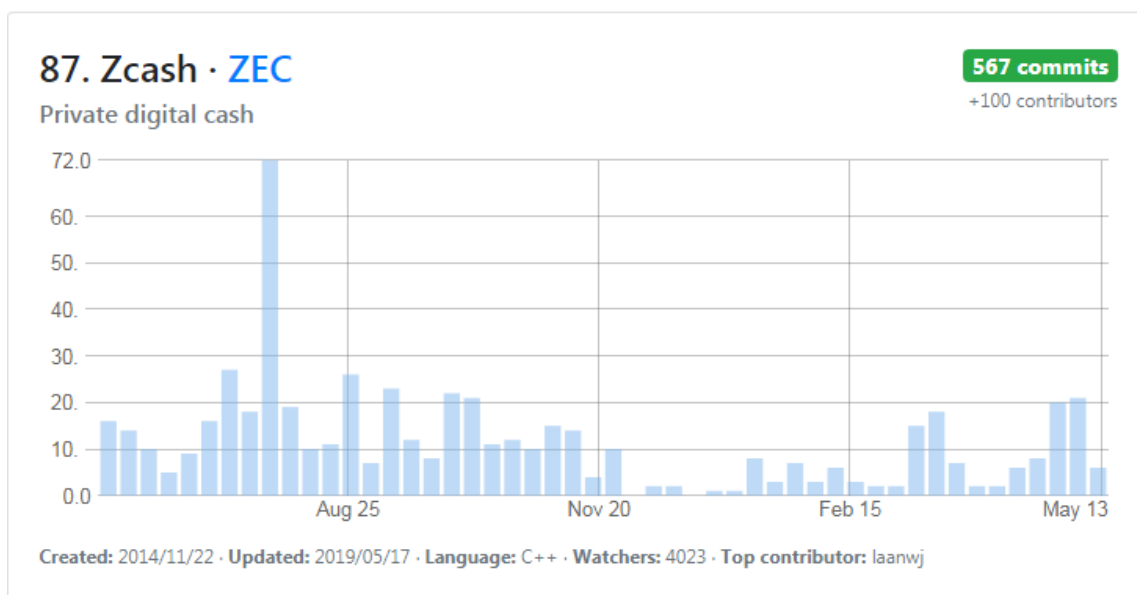
- Konstruowanie prywatnych transakcji przy użyciu zk-SNARKs było niezwykle zasobożerne. Ilość pamięci i czasu potrzebna do takiego procesu, mocno przewyższała jego opłacalność wynikającą z funkcji prywatności. Prywatne transakcje nie mogły być również tworzone za pomocą portfeli mobilnych i sprzętowych. Aktualizacja Sapling zmniejszyła ilość pamięci RAM potrzebnej do konstrukcji zk-SNARK do 40 MB (91% mniej niż poprzednio), zatem jest szansa, że prywatne adresy staną się za jakiś czas standardem. Niemniej, dalsze rozwój w tym kierunku jest potrzebny, ilość pamięci RAM jest nadal na zbyt wysokim poziomie do jakiegokolwiek szerszej adopcji.
- Największe giełdy na których znajdują się pary ZEC/BTC i ZEC/FIAT nie akceptują adresów prywatnych. Mowa między innymi o Gemini, Coinbase i Binance. Zatem nie jesteśmy w stanie upłynnić i wymienić swoich ZEC korzystając z giełd. Głównie z tego powodu, szczególnie górnicy sprzedający wydobyte ZEC, korzystają jedynie z adresów publicznych. Nie korzystają tym samym z żadnych funkcji prywatności oferowanych przez Zcash. Jeżeli polityka giełd nie ulegnie zmianie, a nie ma ku temu żadnych przesłanek, użytkownicy Zcash nadal korzystać będą w przeważającej większości z publicznych adresów. Wiedząc, jak ważną rolę odgrywa ekonomia w kryptowalutach, możemy zakładać, że Zcash nie wprowadzi obowiązkowych adresów prywatnych i tym samym nie stanie się rzeczywiście prywatną kryptowalutą, do momentu, gdy nie powstaną płynne zdecentralizowane giełdy lub obecni liderzy wśród giełd nie zmienią

swojego prawa. Moim zdaniem, regulacje będą się zaostrzać, zatem Zcash będzie musiał w pewnym momencie dokonać wyboru – czy podążamy oryginalną wizją, w której to kryptowaluta ZEC pozostaje prywatna, czy podporządkowujemy się giełdom i regulacjom, aby nie stracić środków na rozwój (opłacenie deweloperów Zcash zależy od kursu kryptowaluty, gdyż pieniądze na to, pozyskiwane są z Funding Reward).

Aktywność deweloperska i audyty kodu Zcash

Dobrym wyznacznikiem rozwoju projektu posiadającego otwarty kod źródłowy jest aktywność deweloperów na platformie Github. Nie sposób zaprzeczyć, że nad Zcash pracuje spora liczba wybitnych naukowców i badaczy, posiadających ogromną wiedzę z zakresu systemów rozproszonych i kryptografii²². Właśnie dlatego skłaniam się ku lepszej ocenie całego projektu, aniżeli wynikałoby to z analizy. Być może jest to błędne podejście, lecz przeczytawszy dziesiątki technicznych dokumentów stworzonych przez zespół pracujący nad Zcash, dochodzę do wniosku, że projekt ma potencjał. Niemniej, jeżeli w badaniach podstawowych nie nastąpi przełom albo nie zostanie wprowadzona inna forma finansowania deweloperów, Zcash mówiąc potocznie, długo nie pociągnie. Najwybitniejszy nawet deweloper nie będzie w stanie przetrwać bez wypłaty!

Spójrzmy więc, jak wykorzystywane są fundusze pozyskiwane z Funding Reward.



Rysunek 21: Aktywność ZEC na platformie Github

²² ECC Team <https://z.cash/team/>

Zcash znajduje się na 87 miejscu w rankingu aktywności kryptowalut. Oczywiście, należy nadmienić, że zazwyczaj kod udostępniany jest w pełnych repozytoriach, a rzeczywiste prace nad nim trwają nieprzerwanie. Mimo to, oczekiwałbym po Zcash większej aktywności.

Za środki pozyskane z Funding Reward, Electric Coin Company – prywatna firma założyciela Zcash, kontrolująca w praktyce całą technologię ZEC, zlecała²³ liczne²⁴ audyty kodu. Najważniejsze z nich, od Kudelski Security²⁵, który przeprowadzał audyt kodu softforku Sapling i ten przeprowadzony przez NCC group²⁶ nie wykazały jakichkolwiek krytycznych błędów. Zwrócono jedynie uwagę na proponowane drobne poprawki. Zatem **pod względem jakości kodu, ZEC jest świetny.**

Wieczny spadek ceny z powodu Funding Reward

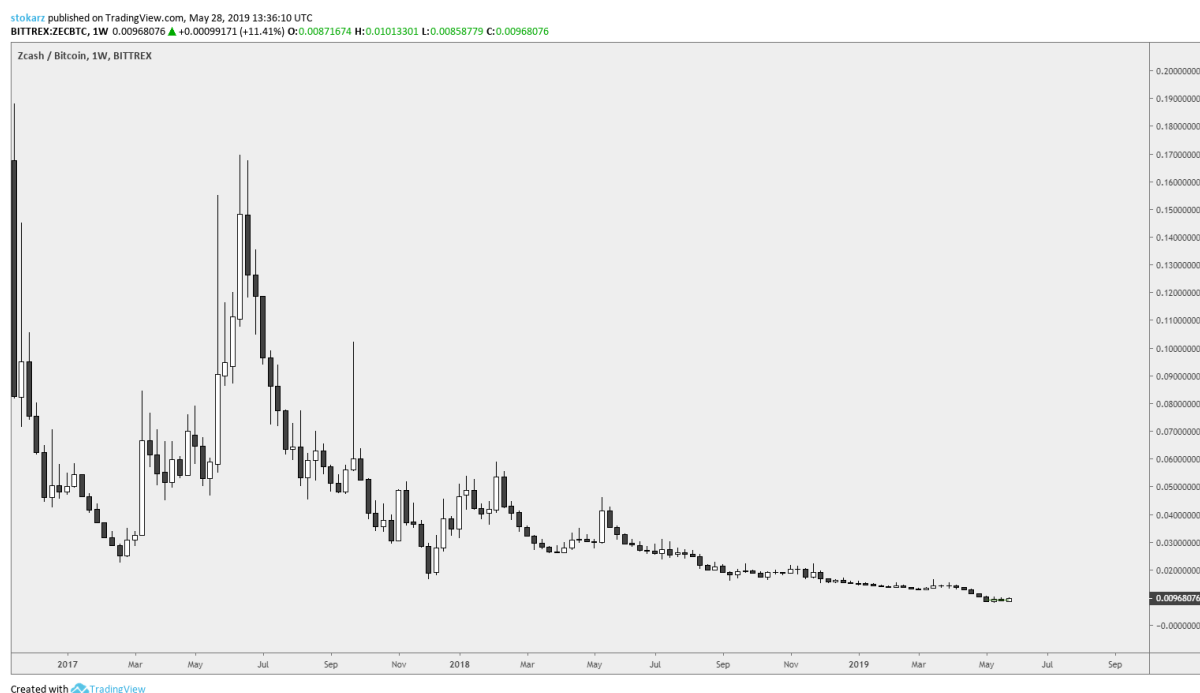
Nie sposób zauważyć, że Funding Reward – 20% ze wszystkich nagród z wydobytych przez górników bloków, trwająca do 2020 – przyczynia się znacząco do wiecznego spadku ceny ZEC. Mało płynne rynki kryptowalut i niewielkie, w porównaniu np. do Bitcoina czy ETH, zainteresowanie ZEC, powoduje, że zarówno górnicy, jak i deweloperzy ZEC, dumpują swoje coiny na rynek. Sprawia to, że od początku istnienia, ZEC znajduje się w jednym wielkim trendzie spadkowym. Jest to wyjątkowa sytuacja, nie spotykana na żadnej z innych kryptowalut.

²³ Audyt kodu Zcash <https://leastauthority.com/blog/zcash-security-audit-reports/>

²⁴ Audyt kodu Sapling <https://medium.com/qed-it/sapling-audit-9b531be9d30>

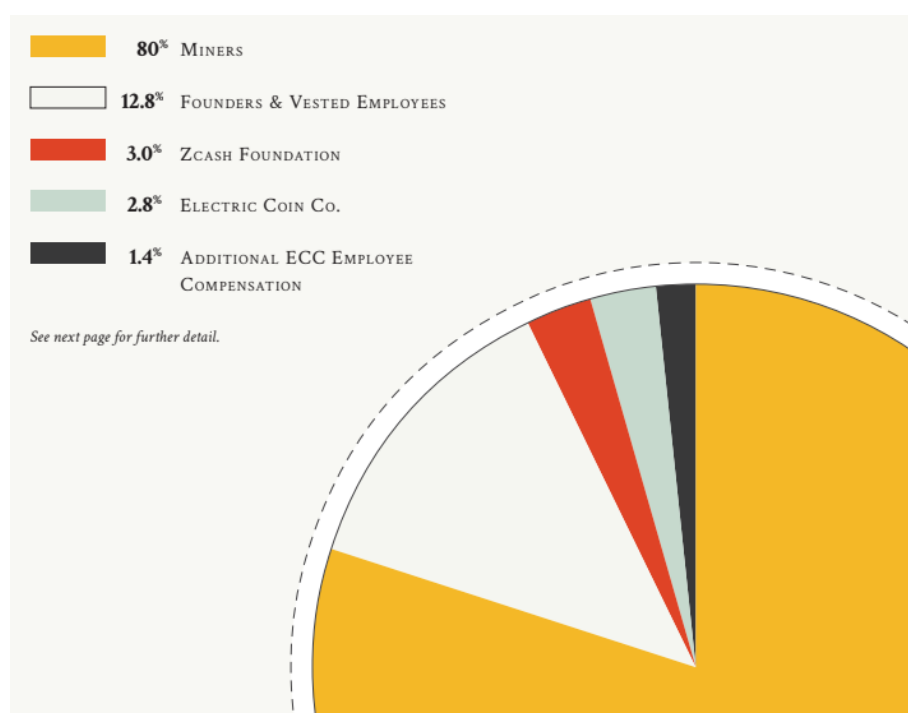
²⁵ Kudelski Security <https://research.kudelskisecurity.com/2019/01/31/audit-of-zcashs-sapling-update/>

²⁶ NCC Group <https://www.nccgroup.trust/us/our-research/zcash-overwinter-consensus-and-sapling-cryptography-review/?research=Public+Reports>



Rysunek 22: Nawet w ciągu bieżącego rynku 2017 roku, ZEC nie był w stanie przebić swojego ATH na parze ZEC/BTC

Aktualna alokacja nagród z wydobytych bloków przedstawiona jest na poniższym wykresie²⁷:



Rysunek 23: Alokacja nagród z wydobytych przez górników bloków

²⁷ ECC Zcash Transparency report <https://z.cash/blog/electric-coin-company-q2-2019-transparency-report/>

Funding Reward przekłada się na określony napływ kapitału, który obrazuje tabela (USD):

RECIPIENT	SHARE OF MINING REWARDS	MONTHLY USD VALUE AT ZEC PRICE OF \$60
MINERS	80.0%	\$10,500,000
FOUNDERS AND VESTED EMPLOYEES	9.6%	\$1,260,000
ZCASH FOUNDATION	2.2%	\$288,750
ELECTRIC COIN COMPANY	5.75%	\$754,688
ADDITIONAL ECC EMPLOYEE COMPENSATION	2.45%	\$321,563

Rysunek 24: Miesięczny dochód z wydobytych przez górników bloków, uwzględniając 20% rozlokowanie Funding Reward

Najważniejsza ze statystyk to ilość kapitału napływająca do Electric Coin Company oraz Zcash Foundation. Pierwsza z tych organizacji jest firmą for-profit i od 3 lat odpowiada za cały rozwój Zcash. To właśnie w niej zatrudnieni są pracownicy ZEC. Jej CEO jest Zooko Wilcox, twórca ZEC. Posiadają oni również wszelkie prawa do technologii Zcash. Sytuacja kapitałowa nie wygląda jednak dobrze. Firma operuje na poważnym deficycie, Funding Reward kończy się w 2020 roku, a jak dotąd, ECC nie znalazło innego modelu finansowania. Aktualna rezerwa kapitałowa wynosi niecałe 5 milionów \$.

Według raportu przygotowanego przez ECC o sytuacji w firmie (przy aktualnej cenie Zcash – w raporcie wycenianego na 60\$), posiadają fundusze na działanie do listopada 2020 roku. Nie wiadomo, jak będzie operowała firma po tym czasie.

Key Takeaways:

- The Electric Coin Company is funded (assuming current price of ZEC) through October 2020.
- The Electric Coin Company and its employees have been receiving approximately 4.2% of the total mining rewards.
- At the current price of approximately \$60 per ZEC, the company and its employees have been receiving approximately \$550k per month.
- The company's operating cost in the second half of 2018 averaged \$700k per month. An additional \$180k a month was used for employee compensation during the period. As such, the company has been running at a significant deficit.
- The Zcash received from the Electric Coin Company's share of mining rewards was used to fund R&D, engineering, global adoption efforts, audits, trademark protections and regulatory relations. The specifics are included in the Expenses and Use of Funds section of this disclosure.
- The company currently holds approximately \$5M worth of USD and Zcash.
- Founders Reward participants recently agreed to a dilution, effective June 2019, to ensure the financial sustainability of the Electric Coin Company.

Rysunek 25: Kluczowe wnioski wynikające z raportu ECC

Electric Coin Company, na chwilę obecną kontroluje niemal cały rozwój Zcash. Czołowi pracownicy ECC podejmują jednak kroki w celu zmiany stanu rzeczy – fundusze jak i kod, i technologia przekazywane są Zcash Foundation – organizacji non-profit, która w przyszłości ma odpowiadać za rozwój projektu Zcash.

Podsumowując: ECC zajmujące się rozwojem Zcash posiada fundusze, zapewniające jej możliwość działania jedynie do końca 2020 roku (jeśli cena Zcash nie ulegnie zmianie). Technologia Zcash jest w rękach prywatnej firmy, ale rozpoczął się proces przekazywania władzy w ręce organizacji non-profit (choć moim zdaniem dzieje się to zbyt wolno). Co więcej, potrzeba finansowania rozwoju projektu, płytki rynek i dumpowanie coinów przez górników – którzy najwyraźniej nie zamierzają Zcash hodlować, wpływa na wieczną dewaluację ceny Zcash w parze ZEC/BTC. Funding Reward przyznawana jest do 2020 roku.



Rysunek 26: Ciekawa opinia Edwarda Snowdena na temat Funding Reward - wnioskuje on, że jest on dobrym rozwiązaniem, gdyż pracownicy ECC z zabójczą prędkością rozwiązują wszelkie napotkane błędy w kryptowalucie. Owszem, jednak cierpi na tym cena ZEC.

Sprzedaż technologii Zcash w celach komercyjnych

W 2018 roku Electric Coin Company sprzedało komercyjną licencję na technologię Zcash amerykańskiemu bankowi inwestycyjnemu – JPMorgan²⁸. Podejmując się współpracy, JPMorgan poszło zadziwiającą wręcz drogą. Wraz z naukowcami ze Stanfordu, opracowało otwarto-źródłowe rozszerzenie prywatnościowe do kryptowaluty Ethereum nazwane Zether²⁹. Technologia ta umożliwia tworzenie prywatnych smart-kontraktów, jest więc ogromnym krokiem naprzód w kwestii prywatności kryptowalut. Docelowo, protokół Zether ma również zostać wbudowany w rozwijany przez JPMorgan prywatny blockchain Quorum.

Sprzedaż technologii Zcash w celu komercyjnego użytku jest jedną z możliwości, dzięki której ECC może pozyskiwać fundusze, jednak takie podejście jest w dużej mierze sprzeczne z tym, czym miał być Zcash – otwartą kryptowalutą zapewniającą prywatność – technologia ta nie powinna być na sprzedaż. Na razie nie widać żadnych negatywnych efektów takiego podejścia – co więcej, Zether stworzony przez JPMorgan i naukowców ze Stanford, długofalowo może

²⁸ JPMorgan Quorum blockchain <https://www.coindesk.com/jpmorgan-adds-new-privacy-features-to-its-ethereum-based-quorum-blockchain>

²⁹ Zether: Towards Privacy in a Smart Contract World <https://crypto.stanford.edu/~buenz/papers/zether.pdf>

wnieść prywatność do Ethereum. Mimo wszystko, preferowane byłoby, aby Zcash nie sprzedawał swojego kodu i technologii w celach komercyjnych.

Podsumowanie

Analiza kryptowaluty Zcash wykazała, że nie jest ona na tyle prywatna, na ile postrzegane jest to przez większą część społeczności. Choć technologia wykorzystywana przez Zcash jest niezwykle zaawansowana i w dłuższym czasie być może nawet rewolucyjna dla finansów i przesyłania pieniędzy, szczególnie w warunkach, kiedy prywatność gra pierwszoplanową rolę, to 95% adresów Zcash nie korzysta z niej. Sprawia to, że pozostałe 5% również jest zagrożone. Drużyna rozwijająca Zcash powinna swe działania skupić na wprowadzenia obowiązkowego wykorzystania adresów typu „z”, dzięki czemu Zcash mógłby stać się naprawdę prywatną kryptowalutą. Konstruowanie zk-SNARKs wiąże się jednak z dużym poborem pamięci RAM, zatem potrzebne są udoskonalenia w protokole, zanim możliwe będzie używanie prywatnych adresów na wysoką skalę. Jednocześnie, w chwili obecnej, Zcash nie powinien być wykorzystywany przez jednostki, których prywatność jest zagrożona, na przykład poprzez wzmożoną kontrolę i inwigilację obywatelską ze strony rządów. Jeśli ECC nie rozwiąże problemu finansowania do końca 2020 roku lub nie doświadczymy potężnego byczego rynku, który spowoduje, że cena ZEC wzrośnie, rozwój Zcash może być zagrożony. Funding Reward i dumpowanie monet przez założycieli i ECC, w celu sfinansowania prac nad ZEC sprawia, że od początku istnienia kryptowaluty, znajduje się ona w trendzie spadkowym w stosunku do BTC. Mimo wszystkich problemów, poznawszy dokładnie zaplecze naukowe jakie posiadają osoby pracujące nad Zcash uważam, że kryptowaluta ma szansę pokonać stojące przed nią trudności i w efekcie zacząć być wykorzystywaną na szeroką skalę. **Jednak konkurencja nie śpi, a kryptowaluty Monero oraz Dash deptają Zcash po piętach. Moim zdaniem, obecny rynek na prywatne kryptowaluty jest na tyle mały, że ta z kryptowalut, która okaże się najbardziej przydatna w środowisku w którym zagrożona jest prywatność, wyprzedzi drastycznie całą resztę – pod względem adopcji i kapitalizacji.**

Zastosowanie Zcash jako narzędzia w walce z obsesją kontroli

Jak dowodzę w artykule: „Przekonam Cię do Bitcoina”³⁰, jedną z pierwszych rzeczy odbieranych przez rządy z obsesją kontroli, jest władza nad pieniądzem. Opisana przeze mnie sytuacja, choć w formie opowieści, ma swoje podłoże w realnej historii ludności zamieszkującej południowe wybrzeże Afryki w XIX wieku i mieszkańców Indii w 1808 roku. W

³⁰ CyberKrypto. Przekonam Cię do Bitcoina.
<https://cyberkrypto.pl/przekonam-cie-do-bitcoina/>

obu przypadkach, Imperium Brytyjskie skonsolidowało swoje władanie nad regionem, poprzez między innymi, odebranie wolności pieniężnej i ustawowym wprowadzeniem funta brytyjskiego, zamiast, używanych od wieków do wymiany towarów, muszli kauri.



Rysunek 27: Wizualizacja chińskiego systemu rozpoznawania - zdjęcie pochodzi z corocznych targów "inwigilacji" w Chinach, na którym takie systemy są prezentowane publicznie

W planie kontroli obywateli realizowanym przez Komunistyczną Partię Chin, możemy dostrzec rażąco podobny schemat. Oprócz tworzenia systemów szpiegowania własnego społeczeństwa, Chiny całkowicie pozbywają się płatności gotówkowych³¹. Zamiast tego, wśród obywateli królują zabójczo proste w użyciu metody płatności za pomocą telefonów i kodów QR od Tencent (WeChat) i Alibaby (Alipay). W każdym z tych przypadków zachowana jest zerowa prywatność transakcji, a całe rejestry finansowe posiadane są przez wyżej wymienione firmy, ściśle współpracujące z chińskim rządem.³²

³¹ Nikkei, Asian Review. In China, cash is no longer king.

<https://asia.nikkei.com/Business/Business-trends/In-China-cash-is-no-longer-king>

³² Japan Times. Worried about Huawei? Take a look at Tencent.

<https://www.japantimes.co.jp/opinion/2019/03/28/commentary/world-commentary/worried-huawei-take-closer-look-tencent/#.XOuchYzaJA>

Moja analiza kryptowaluty Zcash (ZEC) wykazała, że na tą chwilę, **nie powinna być wykorzystywana do walki z kontrolą ze strony organizacji rządowych**, gdyż jej prywatność jest niezwykle krucha i wrażliwa. Zatem może zostać złamana poprzez znających się na rzeczy analityków i w efekcie sprowadzić na jednostkę używającą jej bezpośrednie zagrożenie.

stokarz

Archiwum raportów:

Ambrosus (AMB)

<https://ambrosus.pl/latwe-wejscie-w-blockchain-amb-net-masternode-system/>

NEO (NEO)

<https://www.docdroid.net/bmUvPow/neo-raport-by-stokarz.pdf>

Stellar (XLM)

<https://www.docdroid.net/WS10r86/stellar-konsensus-raport-by-stokarz.pdf>

LSK (LSK)

<https://www.docdroid.net/1PCleep/lisk-lsk-raport-by-stokarz.pdf>

Kanały na platformie Telegram na których się udzielam (@stokarz):

<https://t.me/ArcyTradeAltyczat>

<https://t.me/arocytradebitmexczat>

<https://t.me/CyberKryptoFreedomChat>