i uniwersalnym działaniem ludzi, więc ich największe pomysły z tej właśnie dziedziny wywarły na świat duży wpływ.

Bitcoin: rewolucja pod pseudonimem

Pomysły Satoshi Nakamoto również nie pozostały bez znaczenia, mimo że nikt nie wie, kto to w ogóle jest [108]. 31 października 2008 roku osoba lub grupa ukrywająca się pod tym właśnie imieniem zamieściła w Internecie artykuł *Bitcoin: A Peer-to-Peer Electronic Cash System*, który zajął się odpowiedzią na pytanie: Dlaczego w płatnościach internetowych muszą brać udział banki, firmy kart kredytowych i inni finansowi pośrednicy? Dlaczego nie mogą wyglądać one tak jak płatności gotówką w fizycznym świecie? Transakcje gotówkowe mają bowiem dwie atrakcyjne właściwości: nie wiążą się z nimi żadne opłaty i zachowują one anonimowość płacącego – kiedy płacimy za coś gotówką, zazwyczaj nie musimy się przed nikim legitymować. Fizyczne pieniądze są także długotrwałe i można ich wielokrotnie używać: krążą po naszej gospodarce i cały czas są wykorzystywane, aby za coś zapłacić.

Rządy nie wykazały jak dotychczas zbyt dużych chęci stworzenia cyfrowych dolarów, euro, jenów, renminbi itd. [109] Dlatego też Nakamoto dość ambitnie zaproponował, aby powołać do życia zupełnie nową i niezależną cyfrową walutę o nazwie bitcoin, a ponieważ w dużej mierze opiera się ona na tych samych algorytmach i obliczeniach jak kryptografia (sztuka i nauka tworzenia i łamania kodów), została nazwana ona „kryptowalutą". Amerykańskie dolary, japońskie jeny, tureckie liry, nigeryjskie nairy i wszystkie inne pieniądze emitowane przez narody na całym świecie nazywają się „walutami fiducjarnymi", ponieważ powstały w wyniku dekretu państwowego; rządy po prostu zarządziły, że są one środkiem płatniczym [110].

---

[108] Począwszy od 2008 roku, Nakamoto dzielił się ze światem swoją wizją za pośrednictwem pisanych pod pseudonimem e-maili, postów i elementów kodu źródłowego – wszystkiego, czego potrzebował do zbudowania systemu bitcoinów. Ostatnia publiczna działalność Nakamoto została zarejestrowana pod koniec 2010 roku i od tego czasu kilkakrotnie i bezskutecznie próbowano ustalić jego tożsamość. Jedyne co wiadomo o twórcy bitcoinów, to to, że we wrześniu posiadał lub posiadała niemalże milion BTC (handlowy skrót bitcoinów) wartych ponad 600 milionów dolarów, co stanowi prawie 7% wszystkich bitcoinów w obiegu.

[109] Rządy niektórych krajów zaczęły jednak interesować się cyfrowymi pieniędzmi. Na przykład Bank Anglii ogłosił, że rozpoczyna „wieloletni program badawczy, który ma na celu ocenić główne ekonomiczne, technologiczne i nadzorcze efekty wprowadzenia cyfrowej waluty emitowanej przez banki". Bank Anglii, „Digital Currencies", dostęp: 8 lutego 2017, http://www.bankofengland.co.uk/banknotes/Pages/digitalcurrencies/default.aspx.

[110] Od 1873 do 1971 roku amerykańskie dolary można było wymienić na określoną ilość złota. Amerykański „system waluty złotej" skończył się wraz z serią ekonomicznych zmian wprowadzonych przez prezydenta Richarda Nixona, które przekształciły dolary w walutę fiducjarną.

Istniejące połączenia „kryptokodów" i matematyki pomogły Nakamoto rozwiązać niełatwy problem identyfikacji osób posiadających bitcoiny, ponieważ używa się ich po całym Internecie, aby płacić za różne rzeczy. Użytkownicy wykorzystywali więc swoje cyfrowe podpisy podczas transakcji, aby przekazać odpowiednią ilość bitcoinów od kupujących do sprzedających. Cyfrowe podpisy istnieją już dosyć długo, mają się całkiem nieźle, łatwo je wygenerować, zweryfikować, a za to trudno je podrobić. Ponadto mają one charakter pseudonimu: można wygenerować podpis elektroniczny bez wyjawiania swojej prawdziwej tożsamości. Nakamoto zaproponował również, aby wszystkie transakcje z bitcoinami były zapisywane w katalogu, który rejestrowałby wydawane bitcoiny oraz pseudonimy zarówno klienta, jak i sprzedawcy po zweryfikowaniu ich podpisów.

Jak sprawić, żeby informacje przestały... zachowywać się jak informacje?

Uniwersalny i łatwy w obsłudze katalog był kluczem do tego, aby system bitcoinów radził sobie z kwestią podwójnego wydatkowania (*double spending*). Problem ten pojawił się, ponieważ bitcoiny są wyłącznie informacjami, lecz bardzo ważne jest, aby jednak nie powielały darmowej, idealnej i natychmiastowej ekonomii dóbr informacyjnych, którą omawialiśmy w rozdziale 6. Jeśli bitcoiny mogłyby być kopiowane sposób wolny, idealny i natychmiastowy, to wówczas szerzyłoby się fałszerstwo. Oszuści, kryjący się za swoimi pseudonimami, wydawaliby cały czas te same bitcoiny, dopóki by ich nie złapano, sprzedawcy nie dostawaliby zapłaty, nikt by nikomu nie ufał i cały system bardzo szybko by upadł.

Zaufany i ogólnie dostępny internetowy rejestr rozwiązałby zatem problem double spendingu przez umożliwienie handlowcom (lub komukolwiek innemu) weryfikacji, czy potencjalny nabywca rzeczywiście ma rzeczone bitcoiny i czy nie zostały one już wydane w innym miejscu.

Kto jednak powinien być odpowiedzialny za stworzenie, utrzymanie i zapewnienie spójności tego rejestru? Nie może to być ani bank, ani firma z kartami płatniczymi, ponieważ istota systemu zaproponowanego przez Nakamoto polega na tym, że nie może się on opierać na żadnych istniejących instytucjach finansowych lub na rządach: system bitcoinów musi działać całkowicie niezależnie od nich. Tak naprawdę musiał operować w sposób zupełnie zdecentralizowany (bez odwoływania się do żadnych organizacji lub instytucji) i przetrwać bez względu na to, jak jego użytkownicy będą zmieniać się na przestrzeni czasu. Jak jednak można pogodzić filozofię radykalnej i permanentnej decentralizacji z bezwzględną potrzebą jednego, stałego i wiarygodnego rejestru?