Kryptograficzne aspekty technologii wirtualnej waluty BitCoin

dr inż. WOJCIECH NOWAKOWSKI, prof. ndzw., Instytut Maszyn Matematycznych, Warszawa

Podstawowe określenia

Pieniądz to towar uznany w wyniku ogólnej zgody jako środek wymiany gospodarczej, w którym są wyrażone ceny i wartości wszystkich innych towarów. Jest to materialny lub niematerialny środek, który może być wymieniony na towar lub usługę. *Waluta* jest środkiem rozliczeniowym oraz środkiem regulowania płatności w transakcjach międzynarodowych.

Na pieniądz składają się trzy elementy: *jednostka pieniężna*, *suma pieniężna*, *znak pieniężny*. Podstawowe rodzaje pieniądza to pieniądz *gotówkowy* (pieniądz kruszcowy, metalowy i papierowy czyli monety i banknoty), pieniądz *rozrachunkowy*, czyli bezgotówkowy (czeki, weksle, obligacje, bony, karty płatnicze i kredytowe) i pieniądz *elektroniczny*.

Pieniądz *elektroniczny* czyli *cyfrowy*, został w Polsce zdefiniowany ustawą Prawo bankowe (z dnia 29 sierpnia 1997 roku), jako wartość pieniężna stanowiąca elektroniczny odpowiednik znaków pieniężnych, która spełnia łącznie następujące warunki:

– jest przechowywana na elektronicznych nośnikach informacji, jest wydawana do dyspozycji na podstawie umowy w zamian za środki pieniężne o nominalnej wartości nie mniejszej niż ta wartość,
– jest przyjmowana jako środek płatniczy przez przedsiębiorców innych niż wydający ją do dyspozycji,
– na żądanie jest wymieniana przez wydawcę na środki pieniężne, i
– jest wyrażona w jednostkach pieniężnych.

W prawie Unii Europejskiej istnieje dyrektywa 2000/46/EC Parlamentu Europejskiego i Rady z 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru nad ich działalnością (Dz. Urz. WE L 275 z 27.10.2000 r.). Zgodnie z tą dyrektywą pieniądz elektroniczny jest surogatem monet i banknotów, wartością pieniężną, reprezentowaną przez roszczenie wobec emitenta, przechowywaną na urządzeniu elektronicznym (w postaci np. karty mikroprocesorowej czy pamięci) oraz przeznaczoną do dokonywania płatności elektronicznych. Zwróćmy uwagę, że pieniądz elektroniczny jest *informacją*, a nie bytem fizycznym, jak banknot lub kawałek metalu. W pewnym sensie informacją jest również każdy pieniądz wyrażony w jednostkach, których liczba widnieje na znaku pieniądza, lecz znak ten jest obiektem fizycznym: metalem, papierem lub innym tworzywem.

Pieniądz spełnia cztery główne funkcje ekonomiczne:

– jest środkiem wymiany w transakcjach kupna-sprzedaży. Dzięki niemu mogło nastąpić rozdzielenie w czasie transakcji kupna-sprzedaży na transakcję kupna oraz transakcję sprzedaży, które nie występują jednocześnie,
– jest miernikiem wartości innych towarów w postaci ceny. Aby określić cenę towaru lub usługi nie trzeba posiadać pieniądza, gdyż pełni on rolę miernika wartości również abstrakcyjnie.
– jest środkiem płatniczym, gdy zapłata za towar lub usługę nie następuje jednocześnie z dostawą. Pieniądz spełnia funkcję środka płatniczego również przy realizacji innych zobowiązań, jak np. podatków i opłat, wynagrodzeń pracowników, spłaty kredytów itp.
– jest środkiem przechowywania wartości, czyli *tezauryzacji*. Aby pieniądz prawidłowo spełniał tę funkcję, musi posiadać zaufanie podmiotów gospodarczych i ludności, w szczególności zaś musi przeważać przekonanie, że jego siła nabywcza nie zmniejszy się w znacznym stopniu.

Rodzaje pieniądza

Pieniądzem może być każdy towar, który jest przyjmowany powszechnie w danej populacji jako zapłata za inne towary lub usługi, czyli jest środkiem wymiany. Z wielu względów już w najstarszych cywilizacjach tym środkiem wymiany stał się pieniądz metalowy (kruszcowy). Najpierw były to małe kuliste grudki rzadkiego metalu bądź stopu, z których później bito monety (*rys. 1*).

Rys. 1. Pierwotna moneta z Lidii (cywilizacja grecka, VI w. p.n.e.) ze stopu srebra i złota.
Kwadratowe wgłębienia na rewersie wynikały z niedoskonałej jeszcze techniki bicia. Classical Numismatic Group, Inc., *www.cngcoins.com*
Fig. 1. The original coin from Lydia (Greek civilization, the sixth century BC).
Alloy of silver and gold. On the back double incuse punch.
Classical Numismatic Group, Inc., *www.cngcoins.com*

Monety bito m.in. dlatego, aby nie potrzeba było ważyć kawałków metalu i badać jego próby, czyli sprawdzać ich rzeczywistej wartości. Gwarantem tej wartości był organ emitujący, najczęściej władcy. Narzucali oni monopol bicia monety, również po to, aby odnosić korzyści z procederu psucia pieniądza, właśnie przez zaniżanie wagi i zastępowaniem metalu drogiego – tańszym.

Z czasem, ze względów praktycznych, pieniądz kruszcowy zastąpiono pieniądzem papierowym wymienialnym na kruszec – banknotami, które były dokumentem poświadczającym posiadanie przez emitenta pewnej ilości np. złota. Tylko kilka państw w historii emitowało takie pieniądze, inne nie były w stanie utrzymać odpowiednich rezerw złota, nawet przy częściowej tylko wymienialności. Ostatnią walutą opartą na złocie były do 1971 roku dolary amerykańskie.

Obecnie emitowane są wyłącznie pieniądze *fiducjarne* (łac. *fides* – *wiara*), które nie mają oparcia w dobrach materialnych jak np. kruszce, a są definiowane prawnie jako jedyny legalny środek płatniczy na danym obszarze. Mogą to być pieniądze papierowe, monety bite z metali nieszlachetnych lub monety bite z metalu szlachetnego, lecz o małej względem nominalnej wartości ilości kruszcu.

Pieniądz fiducjarny nie posiada wartości samoistnej, wymaga zaufania do emitenta, czyli w istocie zaufania do państwa, które emituje daną walutę. Podstawową wadą pieniądza fiducjarnego jest to, że można go wygenerować dowolnie dużo. Taka nadmier-

na emisja powoduje inflację, niekiedy bardzo dużą, co podważa zaufanie, a zatem istotę tego pieniądza.

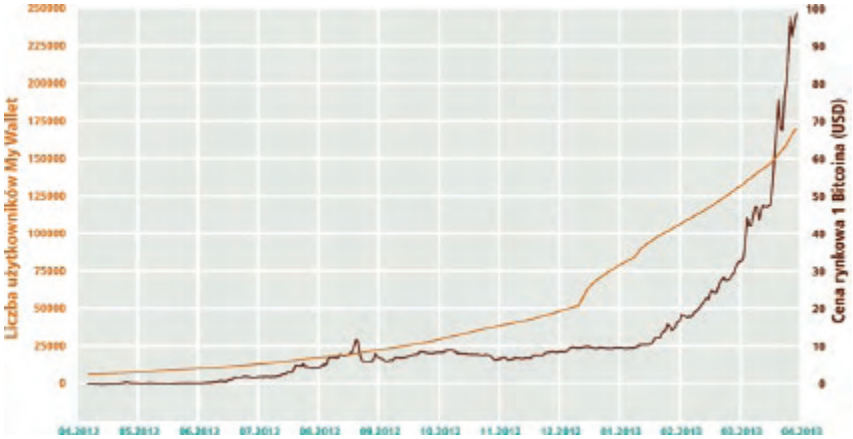
Pieniądze w internecie. Bitcoin (BTC)

Jak już wspomniano, w obrocie międzynarodowym pieniądz (ang. money) określa się walutą (ang. *currency*), zaś określenie *elektroniczny*, czy *cyfrowy* jest zastępowane słowem *wirtualny* (ang. *virtual*). Jeśli obieg waluty wirtualnej zabezpieczany jest technikami kryptograficznymi, to taką walutę nazywa się *kryptowalutą*.

Internet jest globalną i bardzo efektywną siecią przesyłania i wymiany informacji. A ponieważ pieniądz stał się informacją, musiało dojść do licznych prób stworzenia internetowych systemów monetarnych, opartych na wirtualnej walucie, w tym także niezwykle atrakcyjnych dla użytkowników systemów niezależnych od władz i administracji państwowych.

Powszechnie stosowane metody płatności internetowych, np. przelewy z konta bankowego czy płatności kartą polegają bowiem na uprzednim utworzeniu bezpiecznego kanału, chronionego różnymi hasłami i odpowiednimi protokołami. Oczywiście taki kanał zawiera wszystkie dane użytkownika, które są przechowywane w zasobach banku lub podobnej instytucji zapewniającej dostęp do konta. W sieci *Bitcoin* nie ma banku, nie ma chronionych kanałów informacji, nie ma stałych kont. Przesyłane informacje, czyli transfery finansowe, muszą być więc zakodowane, gdyż wchodzą w sieć publiczną. W tym celu w systemie używa się algorytmów symetrycznych z kluczem publicznym i prywatnym oraz funkcji skrótu (tzw. *hash,* dokładniejszy opis podano w rozdziale Zasada działania), a więc podobnej technologii kryptograficznej, jaka jest wykorzystywana w procedurach podpisu elektronicznego [8].

Rys. 2. Podstawowa wersja logo Bitcoin [6]
Fig. 2. Bitcoin currency logo [6]



Rys. 3. Parametry waluty Bitcoin w okresie ostatnich 12 miesięcy (wg. blockchain.info/pl/)
Fig. 3. Bitcoin currency parameters over the past 12 months (blockchain.info/pl)

Bitcoin jest jedną z pierwszych implementacji pomysłu kryptowaluty, opisanego w 1998 r. przez Wei Dai na liście mailingowej *cypherpunków* [1]. Jest to waluta wirtualna sformułowana pierwotnie w 2009 r. przez osobę o pseudonimie Satoshi Nakamoto [2] (nie jest wiadome, czy *Satoshi Nakamoto* to nazwisko konkretnego człowieka, czy też pseudonim grupy programistów, powiązanej, jak się domniemywa, ze środowiskiem hakerskim). Nazwą *Bitcoin* określa się także oprogramowanie typu open *source* oraz sieci *peer-to-peer* (P2P), którą to oprogramowanie formuje. Wirtualne pieniądze, *bitcoiny* (po spolszczeniu *bitmonety*), w skrócie literowym jednostki – *BTC,* mogą być zapisane w pliku na dysku komputera właściciela, w tzw. portfelu (*Bitcoin Wallet*) lub przetrzymywane w zewnętrznym serwisie. W każdym z tych przypadków mogą one zostać przesyłane przez Internet do innych osób, które zainstalowały klienta *Bitcoin,* z podobnym portfelem. System ten nie opiera się na zaufaniu względem centralnego emitenta, ale na wykorzystaniu zdecentralizowanej bazy danych w węzłach sieci *peer-to-peer* oraz zaawansowanych technik kryptograficznych w celu zapewnienia podstawowych funkcji bezpieczeństwa. W oprogramowaniu zakodowany jest na stałe mechanizm kontroli inflacji, znany od początku wszystkim uczestnikom systemu, którego celem jest stopniowe wyemitowanie z góry określonej i nieprzekraczalnej liczby jednostek waluty. Generacja odbywa się losowo, na komputerach użytkowników, według ściśle określonego terminarza. Topologia sieci oraz brak centralnej administracji uniemożliwiają z kolei manipulację wartością waluty jakiejkolwiek rządowej, czy innej organizacji lub jednostce. Możliwa jest jednak bańka spekulacyjna, ponieważ kurs waluty podlega normalnej grze rynkowej. Sieć *Bitcoin* zapewnia prawie anonimowe posiadanie własności oraz jej transfery.

Odmiennie niż w przypadku konwencjonalnej waluty fiducjarnej, Bitcoin nie pozwala żadnemu nadzorcy kontrolować waluty ze względu na swoją zdecentralizowaną naturę.

Przelewanie płatności jest prostsze niż w systemach bankowych. Każdy użytkownik jest anonimowy, nie musi używać ani podawać żadnych danych osobowych, może też używać dowolnej liczby kont. Walutę można nabyć na sposób pierwotny – poprzez wygenerowanie nowych *bitcoinów* lub wtórny – poprzez ich nabycie w drodze wymiany bądź darowizny. Nie istnieją w systemie jakiekolwiek organy zarządcze czy kontrolne. Cała konstrukcja ma charakter czysto publiczny i nie istnieją podmioty, które byłyby w jakikolwiek sposób uprzywilejowane. Emitentem, rejestratorem i posiadaczem jest każdy użytkownik systemu.

Na niezwykle szybki wzrost zainteresowania walutą Bitcoin, zarówno potencjalnych użytkowników, jak i środków przekazu miał niewątpliwie ostatni (2013) kryzys finansowy i zamknięcie banków na Cyprze. Kurs waluty *Bitcoin* jest swobodny i zależy jedynie od relacji popytu i podaży. Jakie były zmiany kursowe tej waluty w ostatnim okresie pokazano na *rys. 3.*

Bitcoin a władze

W ostatnich latach nastąpił żywiołowy rozwój internetowych środków międzynarodowej wymiany i płatności. *Litecoin, e-Gold, Terracoin, NameCoin, Solidcoin, Devcoin, Ixcoin, Namecoin, Ppcoin,* to tylko część listy wirtualnych środków płatniczych, powołanych w sieci przez różne firmy i jednostki. Ze względu na mikroobroty i małe rozpowszechnienie, były one traktowane raczej jako niezbyt groźne zabawy w sieci. Choć wystąpiły zagrożenia, zostały szybko usunięte. Np. w 2007 roku świat obiegła informacja, że

jedna z wirtualnych walut *Linden dollars*, stworzona przez firmę Linden Lab., właściciela portalu wirtualnej rzeczywistości *Second Life*, była przedmiotem nielegalnego hazardu oraz prania brudnych pieniędzy. Firma Linden Lab. miała jednak wszelkie niezbędne środki aby skutecznie zareagować i zablokowała możliwość uprawiania hazardu w *Second Life*.

Dopiero w 2011 roku, gdy nastąpiło powszechne zainteresowanie wirtualną walutą o nazwie *Bitcoin*, skutkujące dużym wolumenem transakcji i liczbą użytkowników, nastąpiła zmiana sytuacji. Zarówno przedstawiciele administracji finansowej USA jak i UE podjęli próbę analizy zjawiska i wydały odpowiednie dokumenty, zresztą o charakterze wstępnym pod względem legislacyjnym.

Przed rokiem 2009 nie istniał pieniądz elektroniczny niepodlegający żadnemu organowi. Nawet sam Internet, uznawany jako zdecentralizowany, ma adresy pod kontrolą. Wszelkie prawa dotyczące walut wirtualnych mogły być egzekwowane przez organ emisyjny, który mógł zamrażać konta użytkowników, doprowadzać do inflacji nadmierną emisją itd. W przypadku wirtualnej waluty *Bitcoin* tak nie jest: nie istnieje żaden centralny organ ani podmiot sprawujący kontrolę. Nawet grupa programistów pracujących nad oprogramowaniem *Bitcoin* nie ma wpływu na sposób funkcjonowania systemu. Jeżeli pojawiłyby się podejrzenia, że system ten mógłby być wykorzystany do maskowania i ukrywania zysków z handlu narkotykami lub prania brudnych pieniędzy, to nie byłoby obecnie wiadomo, względem kogo egzekwować prawo.

Pierwszą poważną oficjalną publikacją dotyczącą walut wirtualnych była obszerna analiza *Virtual currency schemes* [3] opublikowana w końcu 2012 roku przez Europejski Bank Centralny. Jakkolwiek bank ten uważa, że wirtualne waluty nie są w stanie konkurować z Euro, to jednak ich gwałtowny rozwój i niejasny status prawny sprowokowały analizę problemu.

Autorzy tego raportu przyjmują, że waluty wirtualne mogą być powiązane z realną gospodarką na trzy sposoby:

1. Systemy zamknięte. Istnieją w oderwaniu od zewnętrznego świata, obejmując np. rzeczywistość komputerowej gry, gdzie np. wirtualne złoto można zdobywać wewnątrz gry, ale dokonywanie nim transakcji poza grą nie jest dozwolone.
2. Systemy z jednokierunkowym przepływem środków. Taką wirtualną walutę można nabywać za rzeczywiste pieniądze po ustalonym kursie, ale nie jest możliwa transakcja odwrotna.
3. Systemy z dwukierunkowym przepływem środków, gdzie wirtualna waluta może być wymieniana na inne waluty bez ograniczeń. Rolę wejścia i wyjścia pełnią giełdy, kantory i innego rodzaju pośrednicy. Ten rodzaj wirtualnej waluty reprezentuje właśnie *Bitcoin*, wokół którego rozwinęła się cała infrastruktura: od elektronicznych kantorów począwszy, na fizycznych banknotach skończywszy.

Bitcoin pod pewnymi względami jest podobny do pieniądza elektronicznego, nie podlega jednakże dotąd, jak już wspomniano, regulacjom prawnym obejmującym instytucje płatnicze, instytucje pieniądza elektronicznego i instytucje kredytowe. EBC zauważa, że w warunkach skrajnych może pojawić się efekt wypierania „realnego" pieniądza przez wirtualną walutę. Jeśli zastąpi ona w codziennych transakcjach gotówkę i pieniądz bezgotówkowy, to bilans banku centralnego skurczy się, co z kolei wpłynie na jego zdolność prowadzenia polityki monetarnej. Utrudnione stanie się także mierzenie podaży pieniądza.

18 marca 2013 r. *US Department of the Treasury*, a ściślej *The Financial Crimes Enforcement Network* (FinCEN) wydał wytyczne FIN-2013-G001 [4], interpretujące stosowanie przepisów wykonawczych do ustawy Bank Secrecy Act (BSA) do osób emitujących, przyjmujących lub dokonujących obrotów walutami wirtualnymi. Wytyczne przeciwstawiają walutę będącą prawnym środkiem płatniczym w USA lub jakimkolwiek innym kraju, walucie wirtualnej, która działa jak substytut prawdziwej, ale nie ma jej wszystkich atrybutów, w szczególności statusu prawnego środka płatniczego. Z wytycznych tych wynika, że istniejące amerykańskie ustawy, takie jak BSA, nie dotyczą zwykłych użytkowników wirtualnych walut, w tym osób, które generują środki wirtualne. Mogą więc oni dokonywać zakupów lub sprzedaży towarów i usług za ich pomocą. Jednakże jeśli ktoś zajmuje się wymianą wirtualnych na pieniędze umocowane prawnie, lub świadczy usługi ich transferu, powinien mieć licencję i liczyć się z kontrolami FinCEN, które sprawdzać będą, czy wszystkie transakcje są udokumentowane i zgłoszone odpowiednim organom.

Wytyczne nie mają więc większego wpływu na same wirtualne waluty, raczej na osoby i firmy, które na terenie USA zajmują się usługami związanymi z nimi. Są natomiast pierwszym ważnym dokumentem, legalizującym użytkowanie walut wirtualnych.

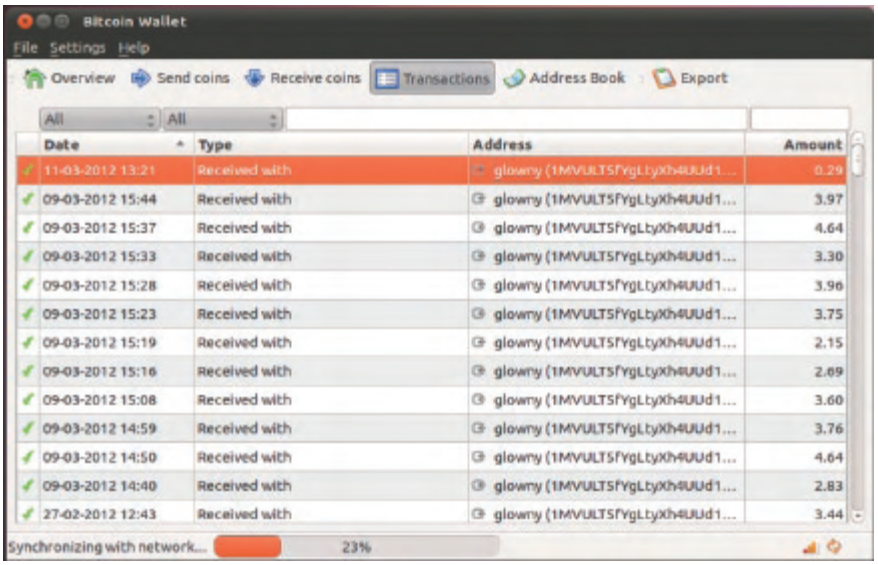
System *Bitcoin* nie daje w gruncie rzeczy ścisłej anonimowości transakcji, gdyż pełna ich historia jest publicznie dostępna. Bardzo trudno dostępna, ale jednak. *Bitcoin* zapewnia natomiast pseudoanonimowość. O ile bowiem łatwo można zindentyfikować tych użytkowników, którzy korzystają z usług wymagających podawania chociażby numerów kont bankowych, to już tych, którzy działają bez podawania danych osobowych zidentyfikować bardzo trudno. W kwietniu 2012 roku FBI wydało dokument [5], w którym przyznano, że połączenie sieci P2P i kryptografii sprawiło, że nowa waluta stanowi dla nich znacznie większe wyzwanie, niż dotychczasowe e-waluty. Raport wspomina o możliwościach pasywnego namierzania uczestników transakcji poprzez analizę łańcucha bloków transakcji, adresów IP i wymienianych przez użytkowników publicznie kluczy publicznych, ale też wymienia sposoby na utrudnienie identyfikacji. FBI ostrzega także przed cyberprzestępcami, którzy mogą okradać użytkowników *Bitcoina*.

Raport FBI opublikowano wtedy, gdy obroty tej waluty szacowano na ok. 40 mln dolarów. Dziś te obroty szacuje się na setki miliardów dolarów. Jest więc prawdopodobne, że z nowej finansowej usługi internetowej korzysta już wielu kryminalistów, wykorzystujących kryptograficzną walutę do prania pieniędzy, handlu ludźmi, sponsorowania terroryzmu, internetowego hazardu czy nielegalnej pornografii. Warto jednak zauważyć, że przestępcy od tysięcy lat znają inny środek płatniczy, umożliwiający anonimowe przekazywanie sobie pieniędzy. To gotówka, za którą można zupełnie anonimowo kupić broń, narkotyki i niewolników. Nie wiadomo co dla zawodowych przestępców będzie lepsze do zaakceptowania: kłopotliwy transfer, czy obawa przed choćby hipotetyczną możliwością kontrolowania ich kryptotransakcji przez administrację. Delegalizację systemu *Bitcoin* należałoby więc zacząć od delegalizacji obrotu gotówkowego

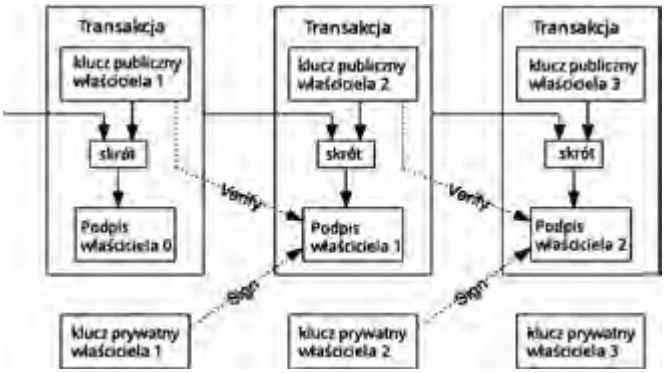
Zasada działania kryptowaluty *Bitcoin* (BTC) [2, 7, 9]

System *Bitcoin* realizuje transfery kwot między publicznymi rachunkami używając kryptografii klucza publicznego. Wszystkie transakcje są publiczne i przechowywane w rozproszonej bazie danych. W celu zapobieżenia podwójnym przelewom tej samej kwoty, sieć implementuje rodzaj rozproszonego serwera czasowego, używając łańcuchowych dowodów matematycznych wykonanych działań (tzw. *dowodów wykonanej pracy*, ang. *Proof of Work*, w skrócie *PoW*). Dlatego też cała historia transakcji musi być przechowywana w bazie, a w celu ograniczenia rozmiaru bazy używane jest drzewo funkcji skrótu (*hash*).

Każda osoba przystępująca do sieci *Bitcoin* instaluje na swoim komputerze program kliencki, który generuje portfel (*Bitcoin Wallet*) zawierający dowolną liczbę par kluczy kryptograficznych. Klucze publiczne, zwane też *adresami bitcoin*, działają jako miejsce źródłowe oraz miejsce docelowe dla wszystkich płatności.



Rys. 4. Portfel użytkownika *Bitcoin* (bitcoin.pl/jak-zaczac/95-tradycyjny-klient-bitcoin)
Fig. 4. Bitcoin user wallet (bitcoin.pl/jak-zaczac/95-tradycyjny-klient-bitcoin)



Rys. 5. Schemat transakcji w systemie *Bitcoin* [2, 7]
Fig. 5. *Bitcoin* transactions diagram [2, 7]

Odpowiadające im prywatne klucze autoryzują płatności tylko dla posiadającego je użytkownika. Adresy nie zawierają żadnej informacji na temat ich właściciela i są zazwyczaj anonimowe.

Adresy, odpowiadające numerom kont w klasycznej bankowości to ciągi alfanumeryczne o długości około 34 znaków, z wykluczeniem cyfry *0*, wielkiej litery *O*, wielkiej litery *I* i małej litery *i*. Użytkownik może posiadać wiele adresów, nawet do każdej transakcji inny. Może generować nowe adresy bez żadnych ograniczeń. Generowanie nowego adresu jest szybkie – w istocie sprowadza się do wyznaczenia przez program kliencki nowej pary kluczy, publicznego i prywatnego, co nie wymaga kontaktu z resztą sieci. Jest także wykorzystywany do jednoznacznej identyfikacji zapłaty za towar poprzez tworzenie unikalnego adresu *Bitcoin* dla każdej transakcji, ponieważ obecnie sieć nie dopuszcza tytułu przelewu znanego z tradycyjnych form przekazu. Tworzenie jednorazowych adresów wykorzystywanych do pojedynczego celu zwiększa stopień anonimowości użytkownika.

Transfery są wykonywane bezpośrednio, bez używania operatorów finansowych prowadzonych przez osoby trzecie i nie mogą być refundowane. Transakcje przebiegają podobnie jak w technologii podpisu elektronicznego [8]. Każda moneta *Bitcoin* jest podpisana cyfrowo kluczem publicznym ECDSA (*Elliptic Curve Digital Signature Algorithm*) jej właściciela. Kiedy przetransferuje on jakąś liczbę *bitmonet* do drugiego użytkownika systemu, rezygnuje z ich posiadania dodając klucz publiczny tego użytkownika podpisując je własnym kluczem prywatnym. Następnie ogłasza wykonaną przez siebie transakcję w komunikacie wysłanym do sieci P2P (*peer-to-peer)*. Gdy nowy właściciel zechce zapłacić swoją monetą komuś innemu, ponownie podpisuje ją swoim kluczem prywatnym, wykorzystując klucz publiczny nowego właściciela. System tworzy w sieci rejestr wszystkich transakcji od początku istnienia sieci, w postaci tzw. łańcucha bloków (*block chain*), który jest upubliczniany przez zapisanie go do powszechnie dostępnego rejestru.

Każdy blok składa się z nagłówka, odróżniającego go od innych bloków, oraz listy transakcji. Łańcuch bloków powstaje przez ich łączenie: blok *n* wskazuje na blok *n-1* poprzez załączenie funkcji skrótu (*hash*) zawartości bloku *n-1*. Jako że ten blok zawiera w sobie funkcję skrótu bloku *n-2*, to skrót ostatniego bloku w łańcuchu jest zależny od skrótu każdego poprzedniego bloku łańcucha. Można więc zapisać *hash* dla bloku np. 10 wzorem:

$$\text{hash}(\text{blok9} + \text{hash}(\text{blok8} + \text{hash}(\text{blok7} + \text{hash} \ldots)))$$

Jeśli dwa węzły uznają wskazany skrót bloku w łańcuchu, to jednocześnie zgadzają się na wszystkie inne bloki. Dzięki tej własności niemożliwe jest sfałszowanie pojedynczego bloku – unieważniłoby to wszystkie poprzednie. Do odnajdywania odbiorcy waluty sieć *Bitcoin* wykorzystuje funkcję skrótu RIPEMD-160 na publicznej części klucza ECDSA, która służy jako unikatowy identyfikator miejsca, do którego wysyłane są *bitcoiny*.

Sprawdzanie bloków, emisja monet *Bitcoin* [2, 7, 9]

Sieć sprawdza poprawność zastosowanych w transakcji podpisów cyfrowych oraz ilości monet przed jej zaakceptowaniem. Dlatego transakcja rozesłana do innych węzłów nie staje się natychmiast „ważna", dopóki nie zostanie zamieszczona w łańcuchu bloków, oznakowana znacznikiem czasu i potwierdzona. W tym celu każdy generujący węzeł (emitent) zbiera wszystkie niepotwierdzone transakcje. Następnie próbuje obliczyć *hash* tego bloku z określonymi cechami, co wymaga z góry przewidywalnej liczby prób i błędów. Kiedy znajdzie rozwiązanie, ogłasza je reszcie sieci. Węzły otrzymujące nowo rozwiązany blok, sprawdzają jego poprawność przed zaakceptowaniem i dodaniem do łańcucha. Ostatecznie łańcuch bloków zawiera kryptograficzną historię zmian posiada-

nia wszystkich monet, poczynając od adresu ich emitenta, aż po adres aktualnego posiadacza. Dlatego właśnie jeżeli użytkownik spróbuje ponownie wykorzystać wydane wcześniej monety, sieć odrzuci próbę wykonania takiej transakcji.

Problem emisji pieniędzy w startującym systemie cyfrowej waluty musi być starannie przemyślany. Nie ma tu banku emisyjnego, który może kontrolować podaż pieniądza. Z drugiej strony pieniądze muszą się w systemie znaleźć, by mogły zapewnić funkcję wymiany. Algorytm emisji musi stopniowo wprowadzać walutę, nie można jej po prostu rozdać, gdyż w chwili startu nie ma jeszcze komu. Twórca (twórcy?) kryptowaluty *Bitcoin* zaproponował wykorzystanie tzw. funkcji *hashcash* [10] (ang. *the hashcash CPU cost-function*), która może być użyta jako wspomniany *dowód wykonanej pracy* (ang. *Proof of Work*). Pracą jest udział niektórych użytkowników systemu w specjalnie utrudnianej procedurze weryfikacji transakcji, wymagającej dużych mocy obliczeniowych w wyspecjalizowanych stacjach roboczych skonfigurowanych z najbardziej wydajnych procesorów (CPU, graficznych CPU, FPGA itd). W literaturze przedmiotu stosuje się zabawne nazewnictwo, sugerujące podobieństwo generacji monet *Bitcoin* do wydobywania złota. Proces ten nazywany jest kopaniem (ang. *mining*), a program *open-source* do tego służący, to *Miner*. Stacje robocze do „kopania" to „koparki".

Procedura *dowodu wykonanej pracy* polega na wyliczaniu funkcji skrótu SHA-256 dla nowego bloku, tworzonego przez *koparki* nasłuchujące wszystkie nowe transakcje (kupno, sprzedaż, darowizna), które wydarzyły się od utworzenia poprzedniego bloku. Na tym bloku *koparki* uruchamiają algorytm haszujący bazując na poprzednim skrócie, oraz losowo wybranej wartości zmiennej tymczasowej (*nonce*) po to, aby można było utworzyć różne skróty (*hashe*) z tych samych danych. Gdy znaleziony zostaje najmniejszy możliwy *hash*, oprogramowanie rozgłasza, że „wygrało wyścig do następnego ważnego bloku". Wówczas zostaje nagrodzone przez sieć 25 (obecnie) nowymi bitmonetami. Obliczenie skrótu dla określonych danych jest stosunkowo proste, ale algorytm wymaga, aby skrót spełniał określone warunek, np. aby na początku miał określoną liczbę zer. Nie da się przewidzieć z góry, jaka wartość zmiennej *nonce* da odpowiedni wynik. Funkcje skrótu muszą być obliczane tak długo, aż otrzymany wynik będzie dobry. Każdy w sieci może sprawdzić, czy twórca bloku faktycznie go utworzył, czy umieścił w bloku jedynie ważne transakcje i czy podjął dla siebie 25 monet za jego utworzenie. Informacje te dostępne są na stronie *blockexplorer.com.*

Warto zwrócić uwagę na to, że liczenie funkcji skrótu SHA-256 jest potrzebne przede wszystkim do autoryzacji transakcji wykonywanych w sieci *Bitcoin* przez innych użytkowników, a więc potwierdzania transakcji, które miały miejsce. W opisanym rozwiązaniu połączono procedurę autoryzacji i emisji, ponieważ w istocie emisja waluty wynagradza pracę autoryzujacych.

Prawdopodobieństwo tego, iż dany *kopacz* otrzyma partię monet zależy od stosunku ilości mocy obliczeniowej wniesionej do sieci za jego pośrednictwem, do sumy mocy obliczeniowej wniesionej przez wszystkie węzły. *Kopacze* mogą także generować bitmonety grupowo, odpowiednio dzieląc urobek. Węzły w sieci oceniają co dwa tygodnie, ile bloków zostało stworzonych, i niezależnie od siebie modyfikują trudność takiej operacji *kopania* tak, by średnio dla całej sieci jeden blok powstawał co 10 minut. W ten sposób ograniczana jest podaż pieniądza bez udziału centralnego serwera. Zgodnie z zaszytą w oprogramowaniu procedurą, liczba możliwych do „wykopania" *bitmonet* zmniejszy z się z upływem czasu do zera tak, by łącznie nie było ich więcej niż 21 milionów. Nastąpi to w 2136 roku.

Już obecnie wysyłający transfery pieniężne w sieci *Bitcoin* mogą wnosić niewielką opłatę transakcyjną. Nie jest to obowiązkowe, ale przyśpiesza autoryzację transakcji, gdyż zachęca kopaczy do uruchamiania oprogramowania generującego, zwłaszcza, że stopień trudności *kopania* na ogół rośnie, a urobek z czasem spada. Węzły zbierają opłaty transakcyjne powiązane ze wszystkimi transakcjami zawartymi w ich bloku. Minimalna opłata transakcyjna za transakcje niskiego priorytetu wynosi obecnie 0,0005 BTC. Zakłada się, że po zakończeniu emisji węzły weryfikacyjne będą utrzymywać się wyłącznie ze zbierania opłat transakcyjnych.

Zakończenie

W przeciwieństwie do innych elektronicznych walut, takich jak *WebMoney* czy *e-gold*, *Bitcoin* jest walutą samą w sobie; w żaden sposób nie ma gwarantowanej ceny ani zapewnionej wartości przez jakiegokolwiek emitenta [11]. Dziś może być wart 120 złotych, jutro 12 groszy lub 1200 PLN. Uważa się, że giełdy walutowe oraz serwisy o przeznaczeniu hazardowym, będące często nielegalne przy rozliczeniach w dolarach, w przypadku korzystania z bitmonet nie podlegają jakimkolwiek regulacjom. To przekonanie wynika stąd, że bitmonety, z prawnego punktu widzenia są niczym innym jak odpowiednikiem pieniędzy stosowanych w grach komputerowych, a ich wartość jest umowna.

Wiele osób uważa, ze *Bitcoin* znalazł zastosowanie jako waluta zupełnie przypadkowo i gdyby nie ogólnoświatowy kryzys, jego wykorzystanie mogłoby być zupełnie inne, ponieważ sam protokół daje nieograniczone możliwości i funkcjonalności. Nie wiadomo, jaki był prawdziwy zamysł *Satoshi Nakamoto*, który uważany jest za twórcę systemu. *Bitcoin* równie dobrze może być wykorzystywany jako zintegrowany system głosowania w wyborach prezydenckich lub parlamentarnych. W gruncie rzeczy *Bitcoin* jest narzędziem do utrzymywania **zsynchronizowanej i zdecentralizowanej, publicznej bazy danych o globalnym zasięgu**.

Czy *Bitcoin* jest walutą? Tony Gallippi (*Co-founder and CEO* w BitPay, Inc.), odpowiada w następujący sposób: *„...owszem, czasami; tak uważa obecnie większość osób. Jednak Bitcoin może równie dobrze pełnić inne funkcje. Czy Bitcoin można traktować jako rejestr księgowy? Zdecydowanie tak. Czy Bitcoin to system barterowy? Być może. Czy Bitcoin jest swoistą bazą danych praw własności? Owszem, jest. Bitcoin może być również wykorzystywany w wielu innych celach."*

Niektóre ze wspomnianych zastosowań stają się obecnie zauważalne. Istnieją np. pomysły na wykorzystanie łańcucha bloków do przechowywania wiadomości. Tony Gallippi uważa, że gdy *Bitcoin* zostanie ustanowiony walutą, inne zastosowania systemu zostaną najprawdopodobniej porzucone. A może jednak nie?

Literatura

[1] http://www.weidai.com/bmoney.txt
[2] Nakamoto S.: Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org/bitcoin.pdf
[3] Virtual currency schemes. European Central Bank, 2012. www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf
[4] FinCEN FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
[5] Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit. Intelligence Assessment. Federal Bureau of Intelligence, 24.04.2012. http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf
[6] https://en.bitcoin.it/wiki/Main_Page
[7] Golański A.: Bitcoin bez płaczu, część 1. Jak działa kryptograficzna e-waluta? webhosting.pl/Bitcoin.bez.placzu.czesc.1.Jak.dziala.kryptograficzna.e_waluta?page=1
[8] Nowakowski W., R. Poznański: Podpis elektroniczny – zasady działania. Elektronika, nr 7/2010, Warszawa
[9] http://pl.wikipedia.org/wiki/Bitcoin
[10] Back A.: Hashcash – a denial of service counter-measure http://www.hashcash.org/papers/hashcash.pdf, 2002.
[11] Szast T.: Bitcoin i regulacje prawne. Portal Paybit, 03.2013. http://paybit.pl/bitcoin-i-regulacje-prawne.