Minimalne Standardy Bezpieczeństwa giełd bitcoinowych

środowiskowe zasady dla rynku giełd kryptowalutowych w Polsce

wersja robocza jedenasta (11 września 2014 r.)

Wprowadzenie

Ponad rok od powstania bloku Genesis w sieci Bitcoin, 5 października 2009 r. ustalono pierwszą wycenę cyfrowej waluty bitcoin na forum internetowym. Od tamtego czasu powstało kilkaset rozwiązań umożliwiających handel bitcoinami. Warto nadmienić, że jedną z pierwszych giełd była polska giełda BitMarket.eu. Powstawaniu kolejnych platform towarzyszyły spektakularne upadki, m.in. jednej z najbardziej popularnych giełd na rynku, MtGox. Upadek giełdy to nie tylko porażka twórców, ale również klientów, którzy powierzają swoje środki giełdzie. Mimo ogromnych postępów, nadal istnieje duże ryzyko, że będziemy mieli do czynienia z kolejnymi przykrymi w skutkach zdarzeniami.

Niniejszy projekt nie kwestionuje praw wolnego rynku, w tym zalet tzw. „twórczej destrukcji", stąd jego celem nie jest zwiększenie stopnia przetrwania giełd na rynku. Jednak cała społeczność bitcoinowa powinna zmierzać do zmniejszenia ryzyka przerzucania konsekwencji upadku giełd na użytkowników. Pomoże to utrwalić na jeszcze wyższym poziomie zaufanie do technologii kryptowalut i zwiększyć ich adaptację w społeczeństwie.

Przewidywany rozwój serwisów giełdowych prowadzi do następującego wyboru:

- pełny liberalizm i akceptacja konsekwencji wolnej konkurencji (tj. dalsze upadki giełd) – z efektami w postaci wolniejszego rozwoju rynku (w tym i podmiotów, które przetrwały), represji ze strony władz publicznych oraz wzrostu strat ponoszonych przez użytkowników; wprowadzone w efekcie regulacje władz publicznych mogą cechować się dużą restrykcyjnością;
- samoregulacja społeczności giełd – dobrowolne przyjęcie, wzorem innych rynków i branż, norm wykonywania działalności gospodarczej i podstawowych standardów mających transparentnie „regulować" rynek.

Oba scenariusze można w tym momencie obserwować na światowym rynku. We Francji regulacją giełd bitcoinowych zajmie się pod koniec bieżącego roku rząd. Już teraz jednak wiadomo, że w planach jest kilka punktów, z którymi społeczność bitcoinowa niekoniecznie się zgadza. W Japonii natomiast powołano grupę, która ma zająć się ustaleniem zasad działania giełd na zasadzie samoregulacji społeczności. W Nowym Jorku na początku 2014 r. podjęto prace nad

licencjonowaniem giełd. Ich efektem jest bardzo restrykcyjna propozycja regulacji (BitLicence).[1] Jej przeniesienie do Polski uniemożliwiłoby funkcjonowanie jakiejkolwiek giełdy bitcoinowej.

Drugie z rozwiązań może być tańsze, mniej kłopotliwe dla giełd, szybsze do wprowadzenia i w efekcie – przyczyniałoby się do przyspieszenia rozwoju całego rynku bitcoinowego w Polsce (i nie tylko).

Cele wprowadzenia unormowań

Cel ogólny: zwiększenie zaufania społeczeństwa do kryptowalut, a w szczególności do giełd bitcoinowych: najpierw w Polsce, później w innych krajach.[2]

Sposób realizacji: określnie minimalnych wymogów bezpieczeństwa, jakie powinien spełniać każdy serwis giełdowy związany z kryptowalutami (dla uproszczenia: z bitcoinem); społeczność byłaby informowana, która z giełd deklaruje[3], że spełnia te minima i w jakim zakresie.

Uzasadnienie: giełdy bitcoinowe, mimo założeń Satoshiego dot. eliminacji trzeciej strony, okazały się być ważnym elementem na styku: pieniądz kryptowalutowy – pieniądz fiducjarny i elektroniczny. By przedostać się do świata kryptowalut, na styku ze światem realnym musiały powstać bramy (*gateways*). Okazały się one być jednak najsłabszym ogniwem przełomowego „projektu bitcoin". Upowszechnienie kryptowalut w dużej mierze zależy od wiarygodności giełd bitcoinowych. Oprócz możliwości osiągania zysków ponoszą one, razem z całą społecznością bitcoina, współodpowiedzialność za rozwój rynku.

Okoliczności: po drugim seminarium bitcoinowym w SGH pt. *„Umarł król, niech żyje król" — bezpieczeństwo nowych giełd bitcoinowych po upadku MtGox* (24 marca 2014 r.) zebrani wtedy przedstawiciele polskich giełd bitcoinowych[4] zgodzili się na wprowadzenie minimalnych kryteriów odnoszących się do bezpieczeństwa, jakie powinna spełniać każda z giełd bitcoinowych. Wprowadzenie standardów w sytuacji oligopolu, podziału rynku między 2-3 funkcjonujące już na rynku podmioty, mogłoby rodzić podejrzenia dotyczące praktyk ograniczających konkurencję. Stąd zapowiedziane w marcu prace nad standardami zostały przesunięte (na lipiec br.).

Metodyka: po wstępnych konsultacjach idei projektu z wybranymi przedstawicielami społeczności, na podstawie informacji o najlepszych praktykach w zakresie bezpieczeństwa zebranych od przedstawicieli giełd w trakcie seminarium, po analizach zapisów na różnych forach internetowych, zaproponowanych zostało prawie 40 kryteriów podzielonych na sześć grup pod kątem tego, jakiego obszaru funkcjonowania giełdy one dotyczą. Mają one mieć postać nie najwyższych możliwych standardów bezpieczeństwa, ale absolutnego minimum, jakie powinno

1 BitLicence, New York State – Department of Financial Services; Proposed New York Codes, Rules And Regulations; Title 23. Department of Financial Services; Chapter I. Regulations of the Superintendent of Financial Services; Part 200. Virtual Currencies; July 17, 2014, http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf

2 Celem tego projektu nie jest przeprowadzenie audytu, świadczenia usług konsultingowych, czy ogólniej – podniesienie zaufania do giełd w wielu aspektach ich funkcjonowania. To pozostaje zadaniem ich zarządów i właścicieli.

3 Kwestia ta jest jedną z największych słabości obecnej wersji projektu – do rozważenia jest przeprowadzenie ew. audytów dla weryfikacji otrzymanych informacji. Zależy to od opinii środowiska giełd.

4 W tym projekty takich serwisów oraz giełdy rejestrowane poza Polską, aczkolwiek realizowane przez Polaków.

być spełnione przez każdy poważny serwis tego typu. Ponadto powinny być one uniezależnione od specyficznych rozwiązań technologicznych (i innych) wdrażanych przez twórców serwisu.

Podstawy prawne: do opracowania poniższego dokumentu wykorzystano m.in. zapisy międzynarodowej normy ISO 27001:2013, nowojorskiej propozycji BitLicence, polskiej Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Niniejsza propozycja standardów nie jest zobowiązująca prawnie.

Kryteria oceny

Na podstawie analiz dotychczasowych największych problemów giełd bitcoinowych, zidentyfikowano sześć obszarów ich działalności, które związane są z szeroko rozumianym pojęciem bezpieczeństwa.

1. **Bezpieczeństwo prawne:**
    - legalność: działalność prowadzona w formie spółki prawa handlowego,
    - transparentność: informacja na stronie internetowej o właścicielach firmy prowadzącej serwis, jej siedzibie, zarządzie, osobach odpowiedzialnych za prowadzenie serwisu oraz sposobach kontaktu,
    - dokumentowanie działalności: przechowywanie i ochrona wszystkich dokumentów oraz zapisów elektronicznych przez okres co najmniej 10 lat[5] od daty ich powstania,
    - porzucona własność: przechowywanie dokumentacji o nieukończonych, zaległych lub nieaktywnych kontach przez okres co najmniej 10 lat[6],
    - ochrona „konsumenta”: regulamin serwisu nie nadużywający przewagi serwisu nad możliwościami ochrony swoich praw przez klientów[7],
    - prawodawstwo: oparcie serwisu na przepisach państwa uważanego za wiarygodnego uczestnika systemu bitcoin (np. kraje OECD, w tym UE),
    - legalność podatkowa: funkcjonowanie serwisu w zgodzie z przepisami podatkowymi,
    - przeciwdziałanie praniu brudnych pieniędzy (AML/KYC)[8]:
        - transakcje ponadprogowe: rejestracja do odpowiedniego organu (w Polsce: Generalny Inspektor Informacji Finansowej, GIIF) transakcji wynikających z dyspozycji klienta, przekraczających wartość 15 tys. euro (również, jeśli posłużono się więcej niż jedną transakcją),

5 Okres ten to czas przedawnienia roszczeń użytkowników będących konsumentami.

6 Wynika to, podobnie jak poprzedni punkt, z art. 118 Kodeksu Cywilnego.

7 W przypadku działalności prowadzonej na terenie Polski: zgodnie z orzecznictwem Sądu Ochrony Konkurencji i Konsumentów.

8 Zgodnie z Ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z 16 listopada 2000 r. (m.in. art. 9d). Zgodnie z nią (art. 2 ust. 1 pkt t) ustawy), instytucją obowiązaną do rejestrowania transakcji są przedsiębiorcy przyjmujący płatności o wysokości 15 tys. euro.

- raporty SAR (*suspicious activity report*): informowanie GIFF o każdej transakcji, co do której okoliczności wskazują na powiązanie z procederem prania pieniędzy,

- identyfikacja klienta: przeprowadzenie weryfikacji użytkownika, jeśli giełda nie dysponuje innymi danymi umożliwiającymi identyfikację klienta przez odpowiednie organy (np. numer konta bankowego lub adres IP[9]) dla transakcji powyżej 1000 euro.

2. **Bezpieczeństwo techniczne:**

- kopie bezpieczeństwa: regularne backupy krytycznych danych [propozycja: minimum co godzinę, w zależności od technologii], szyfrowanie, ew. wysyłanie do innej lokalizacji,
- architektura: możliwe maksymalne oddzielenie serwisu od internetu i zapewnienie bezpiecznego wejścia dla administratorów poprzez odseparowany kanał (inne IP / serwerownia); możliwie maksymalnie restrykcyjne firewalle, wyłączenie / odinstalowane wszelkich zbędnych usług,
- zgłaszanie problemów: posiadanie oddzielnego kanału (adresu e-mail, telefonu itp.) do informowania o zagrożeniach (znaleziony błąd, utrata środków w wyniku błędu serwisu);
- bezpieczeństwo fizyczne serwerów: używanie serwerów (kolokacja / serwery dedykowane / chmura) w możliwie najbardziej wiarygodnych centrach danych oraz zaszyfrowanie ich zawartości (możliwie długimi kluczami), by obsługa centrów nie była w stanie pozyskać z nich danych,
- decentralizacja: utrzymywanie kopii bezpieczeństwa w różnych lokalizacjach,
- szyfrowanie: stosowanie protokołu SSL do szyfrowania połączeń z platformą,
- testy penetracyjne: przeprowadzenie co najmniej raz w roku testów przez jednostki zewnętrzne[10],
- testy obciążeniowe: zmniejszenie podatności serwisu na ataki typu DDoS,
- ścieżka audytu: rejestrowanie wszystkich istotnych operacji od samego początku do zakończenia.

3. **Bezpieczeństwo kryptowalut:**

- *proof of reserve*: cykliczne podawanie do wiadomości publicznej informacji o wysokości środków kryptowalutowych na giełdzie, najlepiej z możliwością weryfikacji prawdziwości informacji przez jednostkę zewnętrzną,
- brak rezerw cząstkowych: jeśli giełda posiada środki innych osób (zabezpiecza, przechowuje, posiada lub utrzymuje nadzór lub kontrolę nad kryptowalutą w imieniu innej osoby), musi posiadać kryptowalutę tego samego rodzaju i w tej samej ilości, jak ta, która jest należna lub zobowiązana tej osobie,

9 Dane z bankowych kart *prepaid*, które mogą być wykorzystywane anonimowo (bez weryfikacji tożsamości) oraz budzące wątpliwości przypadki łączenia się (korzystanie z sieci TOR, z anonimowych proxy), mimo że są one w pełni legalne w Polsce, nie umożliwiają wspomnianej powyżej weryfikacji użytkownika.

10 Propozycja: w przyszłości uwzględnienie przeprowadzania przeglądów kodu źródłowego (jak w BitLicence).

- majątek klientów: zakaz sprzedaży, przenoszenia, przypisywania, wypożyczania, zastawiania pod hipotekę, użycia lub obciążenia w inny sposób majątku klientów,
- dostęp do konta użytkownika: przeprowadzanie dwuetapowej weryfikacji lub innego zabezpieczenia o podobnej wiarygodności,
- proporcje portfeli: posiadanie minimum 80% bitcoinów klientów w zimnych portfelach, z czego 50% powinno być przechowywane w innym miejscu, niż pozostałe[11],
- bezpieczeństwo portfela: przechowywanie zimnych portfeli w bezpiecznej lokalizacji(ach),
- zaokrąglanie: przedstawianie danych finansowych za pomocą liczb całkowitych w miejsce zmiennopozycyjnych.

4. **Bezpieczeństwo finansowe:**

- minimalny kapitał: posiadanie środków własnych (np. na koncie bankowym lub ulokowany w innych, płynnych aktywach) co najmniej w wysokości przeciętnych średniodobowych obrotów serwisu[12] lub odpowiedni kapitał w wysokości regulowanej przez inne ustawy (np. o prawie bankowym);
- zabezpieczenia kontraktów terminowych: uwzględnienie wysokości stosowanej przez giełdę dźwigni finansowej w ustaleniu minimalnej kwoty potrzebnego kapitału własnego, tj. łączna wartość otwartych krótkich pozycji nie powinna przekraczać rezerw własnych posiadanych przez daną giełdę (tj. bez zabezpieczania kontraktów środkami klientów);
- przeciwdziałanie manipulowania rynkiem: monitorowanie bieżących operacji na giełdach w zakresie wykrywania i przeciwdziałania zawieraniu transakcji mogących znacząco zdestabilizować rynek[13] i wprowadzanie odpowiednich działań naprawczych[14];
- fundusz gwarancyjny (rezerwowy): w razie utraty środków kryptowalutowych klientów – możliwość zrekompensowania minimum 50% ich strat,
- dostęp użytkowników do swoich środków: przeprowadzanie regularnych testów obciążenia usług,
- ciągłość funkcjonowania: możliwość zapewnienia środków finansowych w wysokości wystarczającej do zapewnienia ciągłości funkcjonowania serwisu (pokrycia kosztów stałych) przez okres 1,5 roku od uruchomienia działalności.

5. **Bezpieczeństwo organizacyjne:**

- ryzyko osobiste: ograniczona do minimum liczba osób posiadających dostęp do wszystkich środków finansowych giełdy [propozycja: zgodnie z zapisami dot. sposobów reprezentacji w KRS lub brak takiej możliwości],

11 Zimny portfel (ang. *cold wallet*), czyli portfel zawierający jednostki kryptowalut przechowywane *offline*.

12 Lub inne kryterium, które umożliwiłoby pokrycie strat, ale uzależnione od wielkości posiadanych do dyspozycji środków użytkowników.

13 Przykładowo, w skrajnej sytuacji, sprzedaż wysokiej wartości bitcoinów w krótkim czasie w przypadku niskiej płynności rynku, zwłaszcza jeśli w serwisie giełdowym jest zawartych wiele kontraktów terminowych.

14 Przykładem może być tutaj zawieszenie notowań danego waloru (kryptowaluty) w przypadku zachowań odbiegających od normalnego rynku (*orderly market*) obserwowanego na innych giełdach.

- struktura organizacyjna: wyodrębniony dział bezpieczeństwa lub przynajmniej posiadanie do dyspozycji (najlepiej na stałe) osoby/osób mającej/-ych wskazaną w swoich kompetencjach odpowiedzialność za kwestie bezpieczeństwa,
- szkolenia: przeszkolenie każdego z pracowników pod względem bezpieczeństwa (m.in. nt. siły haseł, wykorzystywania prywatnych skrzynek pocztowych, autoryzacji użytkowników).
- awarie: posiadanie pisemnej wersji procedury komunikowania się z wszystkimi istotnymi osobami w razie awarii lub innego zakłócenia działalności,
- wsparcie techniczne: możliwość całodobowego nadzoru technicznego nad serwisem,
- priorytet dla bezpieczeństwa: przyjęcie zasady minimalizacji ryzyka klienta poprzez priorytet dla działań dotyczących bezpieczeństwa, nawet kosztem krótkoterminowych zysków.

6. **Funkcja informacyjna giełdy:**

- okres konserwacji i informowanie o przerwach w działaniu serwisu: nie więcej niż 48 godzin planowanych przerw w dostępie do serwisu średniomiesięcznie oraz informowanie o nich z minimum 24 godzinnym wyprzedzeniem,
- rzetelna informacja: przedstawienie użytkownikom informacji o ryzyku materialnym związanym z korzystaniem z kryptowalut, informacji o warunkach i zasadach korzystania z serwisu oraz przeprowadzania transakcji [propozycja: co najmniej w regulaminie korzystania z serwisu], z wymaganym potwierdzeniem zapoznania się z ww. informacjami przez klienta,
- edukacja użytkowników: posiadanie podstrony serwisu z podstawowymi informacjami na temat serwisu (np. zasady bezpiecznego używania),
- wsparcie użytkownika: pomoc techniczna online (czat lub inne komunikatory) / telefoniczna dostępna w deklarowanych godzinach przez min. 8 godz. dziennie (bez uwzględniania weekendów),
- odpowiedzi dla użytkowników: czas odpowiedzi na maile/zapytania/zgłoszenia poniżej 24 godzin,
- informowanie o awariach: informowanie (drogą mailową oraz poprzez stronę internetową) do wszystkich użytkowników informacji o problemach w funkcjonowaniu serwisu, ogólnej informacji o ich charakterze, planowanym terminie ich rozwiązania, proponowanym postępowaniu użytkowników lub zalecenia dot. unikania pewnych działań;
- edukacja społeczeństwa: podejmowanie działań publicznych na rzecz propagowania rzetelnej wiedzy na temat kryptowalut,
- współpraca środowiskowa: uczestniczenie w inicjatywach wspólnych dla serwisów giełdowych / transakcyjnych, np. wypracowywanie i przestrzeganie standardów bezpieczeństwa, wzajemne informowanie o atakach hackerskich, o nietypowych zachowaniach rynku itp.

Procedura prac

Wiarygodność projektu wymaga transparencji w możliwie wszystkich aspektach. Stąd zarówno wypracowane kryteria, jak i ogólne wyniki powinny być przedstawione do konsultacji polskiej społeczności bitcoinowej: zarówno podmiotów prawnych, jak i użytkowników indywidualnych.

W pierwszej kolejności planuje się osiągnięcie porozumienia środowiska jednostek zainteresowanych przyjęciem standardów. Następnie, w ramach **publicznych konsultacji**, przewiduje się uwzględnienie opinii szerszej społeczności użytkowników bitcoina.

1. **Konsultacje wersji roboczej dokumentu:**
    - eksperci w sprawach bitcoina oraz bezpieczeństwa technicznego,
        - przedstawiciele firm zajmujących się bezpieczeństwem komputerowym,
        - przedstawiciele społeczności bitcoina darzeni autorytetem w kwestiach bezpieczeństwa,
    - następnie: przedstawiciele działających już na rynku polskich giełd – wypracowanie porozumienia i przyjęcie: jednomyślnie lub większością głosów[15].

    Ten etap został zakończony pod koniec sierpnia br.
2. **Po przyjęciu wstępnej wersji dokumentu przez giełdy** odbędą się konsultacje:

    a) z instytucjami publicznymi potencjalnie zaangażowanymi ww. tematyką (m.in. GIIF),

    b) ze społecznością bitcoinową w Polsce. Cel: jawność kryteriów oceny oraz transparentność giełd w minimalnym zakresie bezpieczeństwa.
3. **Wypełnienie** przez giełdy **ankiety** dotyczącej spełnienia (lub nie) Minimalnych Standardów Bezpieczeństwa w oparciu o ww. kryteria.
4. **Ogłoszenie ogólnych wyników ankiet**[16] i wprowadzenie Minimalnych Standardów Bezpieczeństwa, jako środowiskowego rozwiązania obowiązującego (dobrowolnie) serwisy giełdowe.
    - Zebranie opinii społeczności – odniesienie się do oświadczeń giełd przez użytkowników.
5. **Nawiązanie międzynarodowej współpracy** w celu ustalenia podobnych standardów o charakterze międzynarodowym:
    - w pierwszej kolejności: z Blockchain.info i Bitcoin Foundation – zatwierdzenie ogólnych ram badania,
    - ze stowarzyszeniami bitcoinowymi w innych krajach – dostosowanie wymogów do lokalnej specyfiki.

15 Zgodnie z zasadami demokracji proponuje się przyjąć, że Standardy powinny zostać uzgodnione z możliwie wszystkimi z tych podmiotów i zaakceptowane przez większość (propozycja: 51%) tych działających już na rynku.

16 Giełdy będą mogły zastrzec udostępnianie niektórych informacji, jeśli byłoby to podyktowane chęcią wzmocnienia bezpieczeństwa lub względami tajemnicy handlowej.

6. **Ankieta i wprowadzenie Minimalnych Standardów Bezpieczeństwa** na giełdach zagranicznych.
7. **Prace nad rozwojem standardów** – wraz z dojrzewaniem rynku, w tym np. ewentualne przeprowadzanie ratingów giełd i ich instrumentów finansowych.

Autorzy

Niniejszy projekt ma charakter *non-profit*. Realizowany jest przez zespół Instytutu Wiedzy i Innowacji (IWI) pod patronatem Polskiego Stowarzyszenia Bitcoin, przygotowany i koordynowany przez osoby nie związane z żadną z istniejących giełd. Konsultowany jest w środowisku polskiego bitcoina (Polskie Forum Bitcoin, Polskie Stowarzyszenie Bitcoin) oraz wśród specjalistów z innych dziedzin.

Autorzy i konsultanci: bitcoinet.pl* (PFB), Bitmar* (PFB), fun* (PFB), dr Krzysztof Piech (SGH i IWI) – koordynator projektu, Dariusz Jarzębski (IWI), Agata Kotowicz (IWI), Filip Pawczyński (PSB), Izabela Suchocka (IWI), Kacper Wikieł (PFB, Hackerspace Warszawa), dr Konrad Zacharzewski (UMK), Jacek Zemło, Lech Wilczyński (InPay S.A., PSB).

* nickname

Podmioty uczestniczące w konsultacjach: Monetto (Autovaluta), BitBay, Digital Future (serwis Bitcurex), Michau Enterprises Limited (serwis BitMarket).