THE LIGHTNING CONFERENCE

OCTOBER 19-20 BERLIN, GERMANY

Niniejszy dokument jest wyjasnieniem dlaczego w nayszym atm nie wdrozylismy platnosci LN oraz nasz punkt widzenai na przyszlosc LN i co naszym zdaniem winno być w ramach inreastruktury LN umozliwione.

Ale najpierw o naszym doświadczeniu z wdrażaniem LN przy okazji innych projektów, z którym to doświadczeniem pokrótce chcielibyśmy się z Państwem podzielić zanim przejdziemy do meritum sprawy

I tak jesteśmy operatorem mało znanej nawet u nas w Polsce giełdy bitcoinowej o nazwie BtcDuke, w której w sumie jako pierwszej giełdzie na świecie zaimplementowaliśmy wpłaty i wypłaty LN. Wygląda to tak:

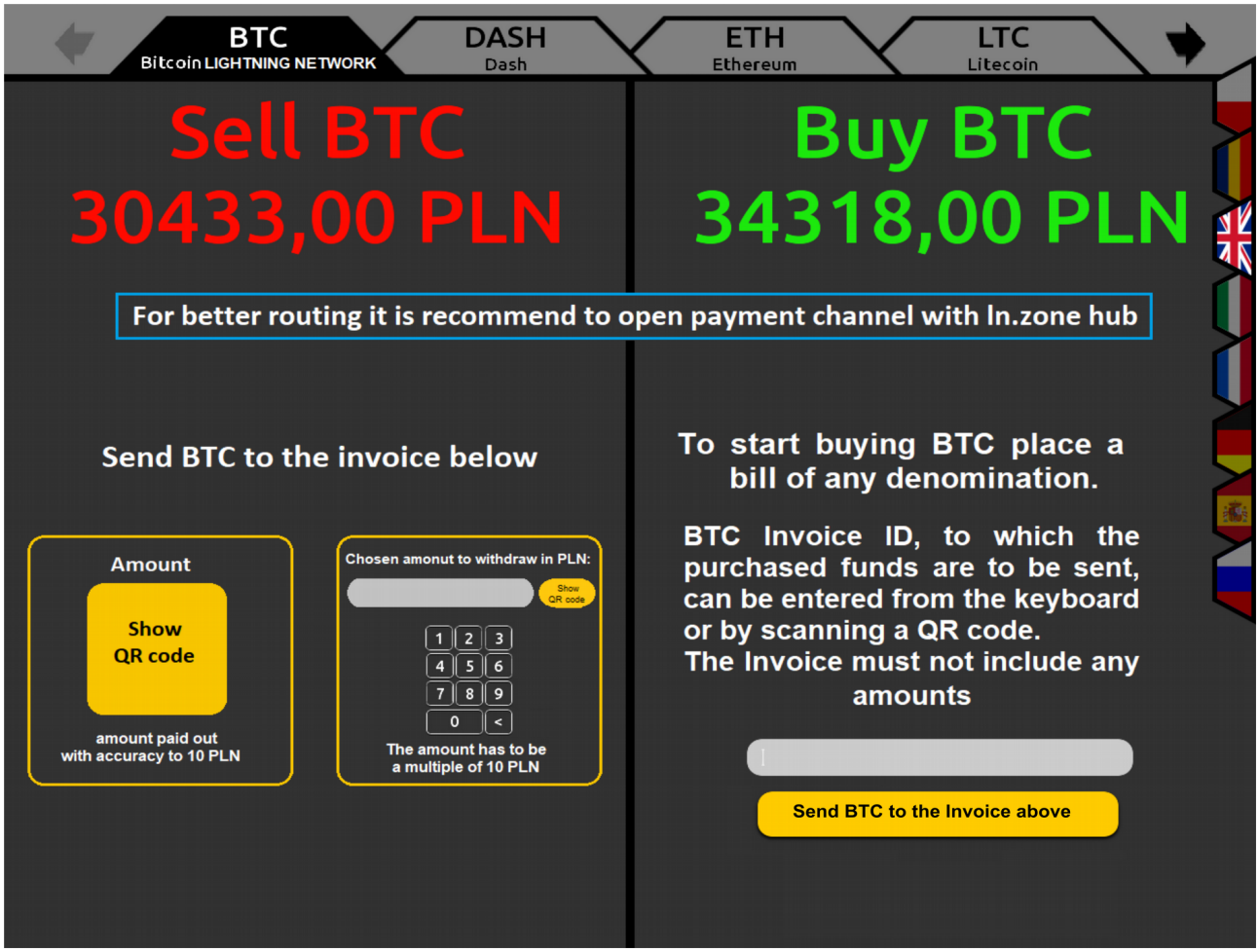
Wypłaty BTC:

Wpłaty BTC:

Nasze doświadczenie w związku z udostępnieniem takiej funkcjonalności klientom, to przede wszystkim to, że gdybyśmy nie wskazali klientom huba, z którym powinni oni otworzyć kanał, to nigdy nie udałoby się nam przerutować do nich płatności – ani od nich do nas ani odwrotnie.

Proszę zobaczyć. Na stronie do obsługi płatności LN zmuszeni byliśmy umieścić dużą wskazówkę z jakim innym węzłem LN, powinni klienci się związać, żeby móc zprzerutować z nami jakąkolwiek płatność. Na potrzeby takiej obsługi klientów zmuszeni byliśmy również stworzyć stronę www dla tego węzła, która to strona umożliwiała klientom otworzenie kanału nie tylko od klienta do tegoż węzła, ale również od węzła do klienta. Z tego co wiemy na te chwile w internecie jest już sporo tego rodzaju witryn. Nasza jest dostępna pod domeną ln.zone.

Kolejnym naszym zamysłem jako fanów LN było wdrożenie tej technologii na naszych bankomatach. Tak miało to wyglądać:



Interfejs do sprzedawania i kupowania BTC za pomocą LN, to miała to być po lewej stronie narzędzie do generowania QR kodu z właściwą kwotą transferu jeżeli ktoś chce nam sprzedać BTC (również za pomocą generowania przez nas invoice bez kwoty), a po prawej narzędzie gdzie sumują się środki pieniężne włożone prze klienta i po zeskanowaniu u nas invoice bez kwoty środki staramy się przesłać klientowi.
Realizując coś takiego mieliśmy w planie w przypadku, kiedy klient chce kupić od nas BTC to w przypadku braku routingu do klienta mieliśmy zamiar wydawać mu specjalne ID transakcji i pozwolić mu spróbować przerutować do niego BTC kiedy indziej – kiedy będzie on związany większą ilością kanałów. Porzuciliśmy te prace jednak ze względu na to, że Bankomaty Bitcoin zarabiają wyłącznie na dużych klientach, dużych transakcjach. LN używają wyłącznie hobbyści wyłącznie w zakresie eksperymentalnych kwot, które zdecydowanie nie pozwolą sfinansować nawet kosztów supportu przeznaczonego dla nich, nie wspominając o pracach programistycznych, dlatego w najbliższym czasie nie zamierzamy wprowadzić LN na naszych bankomatach.

Dlaczego więc mimo to poprosiliśmy organizatorów o możliwość wystąpienia? Dlatego, że jesteśmy przekonani, że wiemy co jest w stanie spopularyzować LN i wydobyć z niego drzemiący w nim potencjał.

A mianowicie jesteśmy zdania, że co najmniej niewystarczająca jest koncepcja, żeby węzły pośredniczące wynagradzane były za rutowanie płatności, a nie – za zamrożone w węzłach z klientami środki. Uważamy, że to co jest w istocie kosztem utrzymania węzła w sieci LN to nie – rutowanie transakcji kosztujące tyle, co prąd zużywany przez maszynę na którym postawiony jest nod. To co jest ograniczeniem w tworzeniu coraz to nowych kanałów, to po pierwsze fakt, że nikt nie może otworzyć dowolnej ich ilości z dowolną ilością innych węzłów, bowiem nikt nie ma nieskończonej ilości BTC, a po drugie co ważniejsze, to jakimkolwiek próbom zaistnienia w tej infrastrukturze poprzez otwarcie kanałów własnymi środkami grożą ataki hakerskie na serwery nodów takiego zapaleńca. Nie należy tego ryzyka lekceważyć bowiem przecież najbardziej nawet poważne giełdy bitcoinowe padały ofiarami ataków. Zdobycie kontroli nad komputerem węzła LN daje identyczne możliwości, co zdobycie kontroli nad komputerem z uruchomionym tradycyjnym nodem sieci BTC.

Tak więc biorąc za przykład osławioną kawiarnię, która pragnęłaby przyjmować płatności w BTC, to prowadzący taką kawiarnie musiałby nawiązać współpracę z hubem płatniczym, który zdecyduje się na otwarcie takiego kanału, w którym po stronie huba będą środki przeznaczone na płatności za kawy. Naiwnością jest sądzić, że ktoś otworzy z nami taki kanał charytatywnie. Przypuśćmy bowiem, że właścicielowi takiej kawiarni wydaje się, że w szybkim czasie sprzeda kaw za aż 1 BTC. Czy ktokolwiek komercyjnie zamroziłby na rzecz tej kawiarni aż 1BTC? Jeżeli właścicielowi kawiarni wystarczy mniej, powiedzmy 0.01 BTC, to co miałby zrobić taki komercyjny hub, jeżeli w krótkiej jednostce czasu zgłosiłoby się do niego 1000 takich klientów deklarujących się jako kawiarnie. Iluś z nich to mogliby być dowcipnisie, a tylko część to osoby na prawdę spodziewające się płatności.

Problemem każdego huba płatności LN będzie,po pierwsze to, że dysponuje on ograniczoną ilością BTC, a po drugie każda kolejna godzina prosperowania takiego huba niesie ze sobą koszt wynikający z ryzyka padnięcia ofiara ataku hakerskiego.

Upieramy się więc, że powinno się dać możliwość węzłom LN implementować interfejs taki, że inne nody mogą się go odpytywać o:

1). stały koszt routowania transakcji (w tej chwili zdaje się 1 Satoshi).
2). dodatkowy koszt routowania transakcji zależy od kwoty transakcji wyrażonej w BTC / BTC (w tej chwili standardowo są to chyba 0.000000001).
3). koszt zamrożenia środków przez HUB-a w kanale wyraźny w BTC/BTC na jednostkę czasu. Za jednostkę czasu uważamy, że najwłaściwszą będzie tutaj jeden blok, z uwagi na to, że użycie innej wiązałoby się z problematycznym zagadnieniem synchronizacji. Gdyby HUB miał zarabiać na zamrożonych środkach, na przykład 10% w skali roku, to liczba ta wynosiłaby zdaje się około 0.0000018. Wydaje nam się przy tym, że kapitalizacja tego wynagrodzenia HUB-a powinna mieć miejsce wraz z wykopaniem każdego kolejnego bloku.
   Przy czym przychody ze współpracy z klientem pochodzące w sumie z 1). i 2). winny odejmowane być od kosztów klienta utrzymywania kanału określonego tutaj

w 3). Jeżeli przychody HUB-a ze współpracy z klientem w związku z 1). i 2). są większe niż z 3). to z 3). nie są pobierane w ogóle. Taka polityka pozwala na współpracę na tych samych zasadach, co opisane tutaj nie tylko pomiędzy HUB-ami i na przykład sklepami internetowymi, ale również na linii HUB-HUB. HUB-a nie musi dzięki temu interesować kto jest podłączającym się do niego klientem: czy jest to kawiarnia akceptująca płatności LN czy inny HUB. Wszystko wychodzi w trakcie współpracy i klienci obydwóch przypadków będą przez HUB mile widzianymi.

4). koszt w BTC HUB-a który liczy sobie za zawiązanie transakcji on-chain otwierjacej kanal oraz zamykającej kanał

Zaproponowane rozwiązanie, że koszty wymienione tutaj jako 3) są pomniejszone o te, które hub „zarobił" na kliencie dzięki rutowaniu jego transakcji powoduje, że model ten idealnie wpisuje się w ew. współpracę hubów komercyjnych.

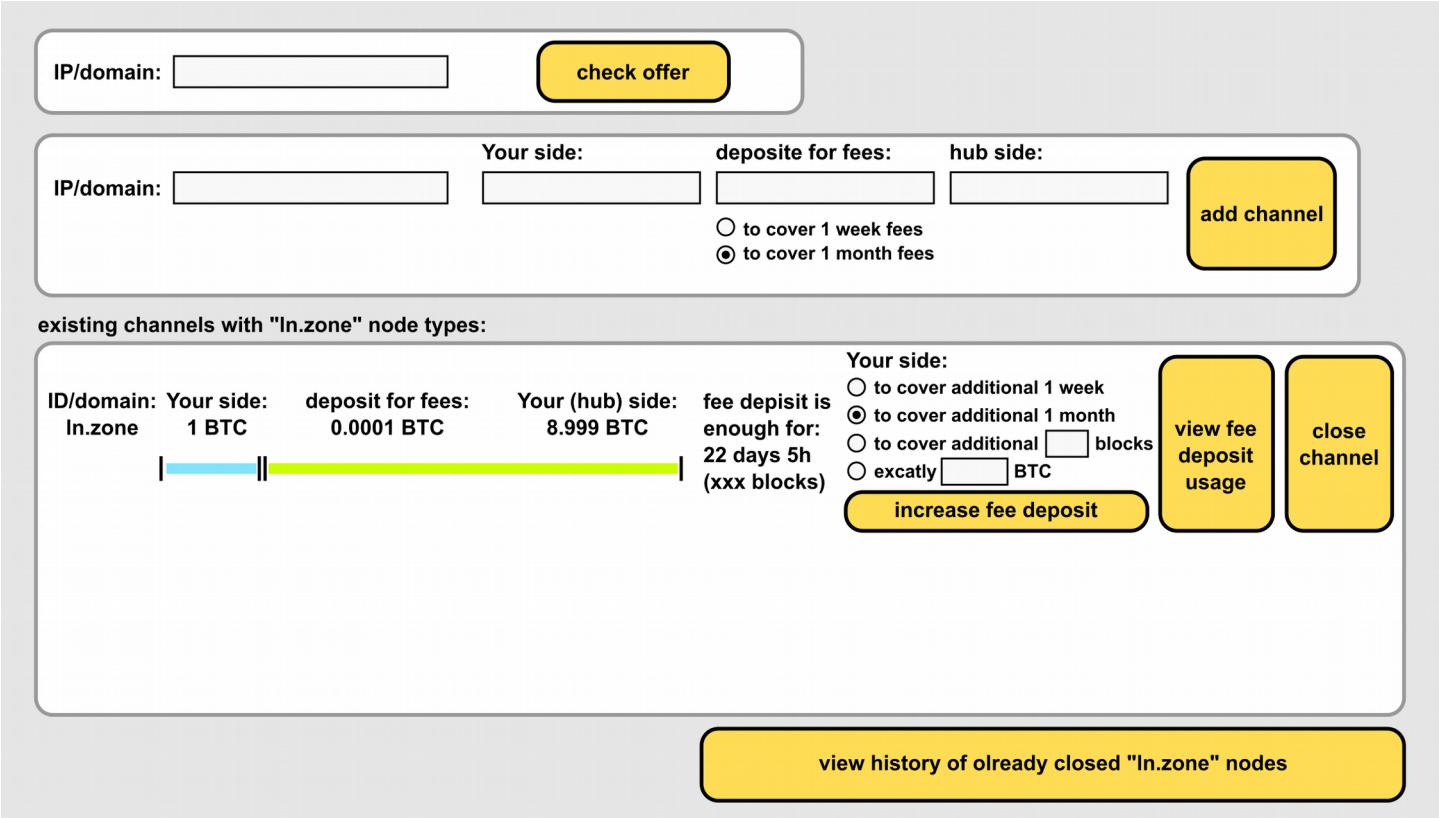
Jeżeliby nie uwzględniać kosztów zamrożenia przez hub środków w kanale, to w zasadzie żaden hub nie zdobędzie się na współpracę z żadnym innym hubem. Nikt bowiem nie zdecydowałby się otworzyć kanał z nieznanym przedsiębiorcą, który w sumie deklaruje ze zapewni ruting wielu transakcji, to nie wiadomo czy się z tego wywiąże. Chęć takiej współpracy mogłoby zadeklarować wiele takich nieznanych hubów i przez to limit BTC tak odpytywanego naszego dużego huba szybko wyczerpałyby się. Dzięki temu, że hub domagający się zamrożenia środków od innego płaci za zamrożenie tych środków dzięki temu, że ew. zyski z rutowania transakcji są odejmowane z tego wynagrodzenia zapewnia sytuacje, że nikomu nie będzie się opłacało odmawiać współpracy z nowo podłączającymi się do sieci.

Niektórzy idealiści LN na taki przedstawiany przez nas punkt widzenia odpowiadają, że przecież owa kawiarnia też będzie musiała płacić za, na przykład towar i całość ruchu LN płatności do kawiarni i płatności realizowanych przez nią się skompensują. Jednak na dzień dzisiejszy kawiarnia za pomocą LN nie zapłaci dosłownie za nic. **To nie jest dobry sposób rozpropagowania systemu płatności poprzez założenie, że z miejsca będzie on jednym na świecie systemem płatniczym**. Nawet zakładając, że sieć LN kiedyś zdobędzie pożądaną przez nas popularność, to naiwnym jest domaganie się, żeby każdy kto w toku prowadzonej działalności gospodarczej potrzebował wydawać w sieci LN tyle samo środków, co ich za pomocą sieci LN przyjmował.

Uważamy, że nie jest konieczne, żeby każdy nod musiał deklarować takie koszty zamrażania przez niego środków, ale uważamy, że taka opcja winna być uwzględniona choćby poprzez możliwości odpytywań noda o wskazane powyżej 4 opcje. Nod chcący zawiązać kanał z takim hubem powinien wyslac hubowi takei zaproszenie do wspolpracy zawierające:

1) jakiej pojemności kanał chce otworzyć z HUB-em;
2) ile w tym kanale ma mieć zamrożonych środków HUB;
3) jaka część z pozostałych środków w kanale normalnie przypisanych klientowi ma być przeznaczona jako depozyt na opłaty dla HUB-a.

Uważamy, że do takiej interakcji noda – klienta (kawiarni) względem huba wystarczyłby interfejs graficzny wyposażony między innymi w widok:

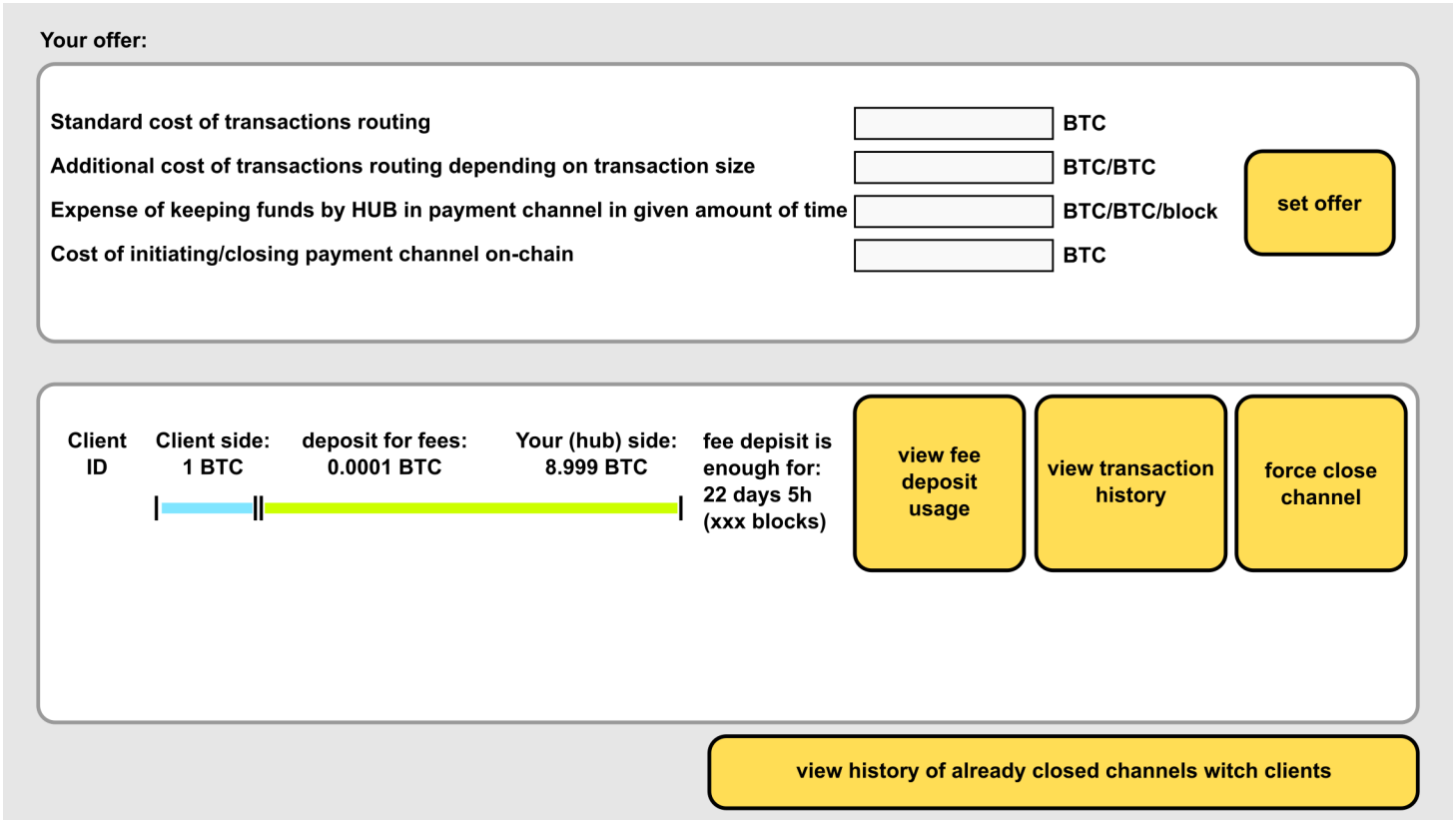


pierwszym przyciskiem u góry sprawdzamy ofertę huba (po jego kliknięciu powinno wyświetlić się okno z ofertą huba), dalej jeżeli się nią zainteresowaliśmy to deklarujemy w prośbie o nawiązanie współpracy trzy dane wymagane celem nawiązania tej współpracy, a następnie otwierany jest kanał, w którym podział środków wygląda tak jak na liście kanałów wskazanych poniżej.
Część środków to środki należące do klienta, część to środki należące do huba. W części środków należących do huba znajduje się mały wycinek tego, co klient pozostawił hubowi, jako depozyt na poczet kosztów utrzymania kanału. Depozyt ten w każdej chwili można odpowiednio zwiększyć (przycisk „increase fee deposit”), za pomocą wbudowanej w portfel opcji zwiększania tego depozytu poprzez transakcje LN pomiędzy klientem a hubem, można też przejrzeć historię użycia tego depozytu, czy zamknąć kanał.

Przycisnięcie przycisku „acc channel” winno skutkowac wysłaniem do huba trzecg zmiennych wymienionych w ostatnim slajdzie, a następnie otworzneiem kanalu dwustronnego. Nie opisujemy tutaj w jaki sposób stworzyć dwustronny kanał. Najlepiej chyba, aby były to w istocie dwa kanały: jeden – pierwszy założony przez klienta do huba. Tuż po otwarciu tego kanału klient przekazuje hubowi poprzez transakcje LN depozyt na fee, a następnie po jego otrzymaniu hub może otworzyć kanał do klienta w wysokości zadeklarowanej wcześniej przez klienta w trzech przeslanych mu zmiennych. Takie rozwiązanie jest trustless i jedynym ryzykiem klienta jest depozyt zabezpieczający na poczet fee. Ze strony aplikacji klienckiej proponujemy ukrywać przed klientem fakt, że ów dwustronny kanał, to w istocie dwa kanały

Taki model płacy gwarantuje hubowi, że w przypadku wyczerpania się depozytu (w powyższym obrazku widać, że w tym wypadku wystarcza on jeszcze na 22 dni), automatycznie zamyka kanał zostawiając klientowi tyle, ile wynosiła wartość kanału po stronie klienta.

Jezeli chodzi o zarzadzania takimi nodem od strony huba, to naszym zdaniem dla huba może być udostepniony widok choćby nastepujacy:



gdzie hub może dekladowac wszystkie interesujace jego potencjalnych klientow informacje.

Powyższy pomysł nie uwzględnia takich niuansów jak to, że hub winien może zmienić swoją ofertę w przyszłości. Można by umożliwiać mu informowania o tym wcześniej poprzez jakieś specjalne zapytanie, o to jak warunki huba wyglądały będą w przyszłości. Hub na takie zapytanie może wskazywać nową ofertę i blok od którego będzie obowiązywała. To ma wyłącznie funkcje informacyjne, bo bub i tak pobiera z depozytu klienta tyle ile mu się podoba, ale przekazywanie tego rodzaju informacji winno być przewidziane.

To w zasadzie wszystko co mamy do zaproponowania

My sami chcieliśmy zaimplementować powyższe tworząc kolejną warstwę ponad LN domagając się zarówno od klientów takiego huba komercyjnego jak i samych hubów uruchamianie kolejnej aplikacji ponad LN. Uważamy to jednak na tyle ważną myślą, że winno być wdrożone w ramach całej infrastruktury LN i do tego deweloperów LN zachęcamy.

Adam Gramowski

shitcoins.club