

Stellar (XLM)

Krytyczny stan centralizacji sieci

02.05.2019

by stokarz

Wprowadzenie

Celem tego opracowania jest przedstawienie obecnego stanu procesu dochodzenia węzłów do konsensusu w sieci Stellar, za pomocą protokołu SCP (Stellar Consensus Protocol) opierającego się na modelu FBA (Federated Byzantine Agreement), jak i zaprezentowanie problemów wiążących się z możliwością blokady sieci w przypadku, gdy zaatakowane zostaną trzy z głównych węzłów zarządzanych przez Stellar Development Foundation. Raport nie obejmuje całościowo projektu Stellar, a jedynie jedną z jego części – fundamentalną architekturę dochodzenia do porozumienia w obrębie zdecentralizowanej sieci.

Raport opiera się w dużej mierze na badaniu przeprowadzonym przez trójkę naukowców z Korei Południowej[1]: Minjeong Kim (KAIST), Yujin Kwon (KAIST), Yongdae Kim (KAIST). Tytuł oryginalny: „Is Stellar as secure as you think?". Reszta wykorzystanych przeze mnie źródeł podana jest w bibliografii.

Wyniki opublikowane w raporcie koreańskich naukowców, doprowadziły do ogólnoświatowej dyskusji[2] pomiędzy deweloperami i członkami społeczności Stellar. Wiele z kryptowalut, choć jawnie twierdzi, że są w pełni zdecentralizowane, w rzeczywistości jest silnie scentralizowana i posiada wiele punktów w które można zaatakować, tym samym wyłączając całą sieć.

Dotyczy to szczególnie kryptowalut opartych o nieefektywne w zdecentralizowanym konsensusie protokoły DBFT i PBFT – używają je np. NEO i Zilliqa oraz kryptowalut wykorzystujących wprawdzie POW, jednak nie posiadających wystarczającej mocy obliczeniowej do efektywnego zwiększenia kosztów ataku sieci przy ataku 51% (kiedy to koszty ataku 51% są na tyle wysokie, aby przestało być to opłacalne ekonomicznie dla jakiejkolwiek organizacji).

Chciałbym, aby również Polska społeczność zrzeszająca miłośników kryptowalut zaczęła zauważać ten problem, gdyż dotyczy on wielu kryptowalut, nawet tych z TOP 10, jak wykazałem w swoim poprzednim raporcie: „NEO – Smart Economy[3]".

Zachowanie zgody między węzłami w zdecentralizowanych sieciach to podstawa. Bez tego, jak inaczej możesz potwierdzić, że kryptowaluta którą przechowujesz jest w rzeczywistości twoja? Satoshi Nakamoto, aby rozwiązać ten problem (a także podwójnego wydatkowania) wprowadził do Bitcoina protokół POW (Proof of Work). Stawia on najwyższą wagę na bezpieczeństwo.

Jednak kolejne kryptowaluty, w celu zwiększenia przepustowości sieci i możliwości propagowania większej ilości transakcji na sekundę, stosują w swoich blockchainach inne sposoby dochodzenia do zgody. Niestety większość z nich prowadzi, lub możliwa jest, jedynie przy znaczącej, lub pełnej centralizacji węzłów autoryzujących transakcje w sieci.

[1] https://arxiv.org/pdf/1904.13302.pdf

[2] https://www.reddit.com/r/Stellar/comments/bblahk/is_stellar_as_secure_as_you_think/?sort=new&depth=1

[3] https://tokeny.pl/neo/

O autorze

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

E-mail: stokarzlol@gmail.com

Telegram: @stokarz

Kluczowe wnioski:

- Analiza mechanizmu konsensusu sieci Stellar - FBA, wykazała, że jeśli bezpieczeństwo systemu FBA ma większą odporność na błędy niż PBFT, to żywotność systemu FBA będzie miała mniejszą odporność na błędy niż PBFT.

- Aktualna konfiguracja FBA wykorzystywana przez Stellar jest silnie scentralizowana.

- Badanie błędów kaskadowych przy obecnej konfiguracji kworum w sieci Stellar wykazało, że jeśli zaatakowane zostaną trzy z najważniejszych węzłów, blockchain Stellar ulega pełnej awarii.

- Trzy z najważniejszych węzłów należą do Fundacji Stellar, tworząc tzw. „single point of failure" – jeden czuły punkt w bezpieczeństwie blockchainu, w który można zaatakować, w celu zatrzymania całej sieci.

- Stellar posiada hierarchiczną strukturę węzłów w sieci. Przeczy to równości i niezależności pełnych węzłów znanej z Bitcoina i Ethereum, które wykorzystują protokół POW (Proof of Work).

- W odpowiedzi na przeprowadzone badanie Stellar Development Foundation podjęła kroki mające na celu zmniejszenie centralizacji sieci.

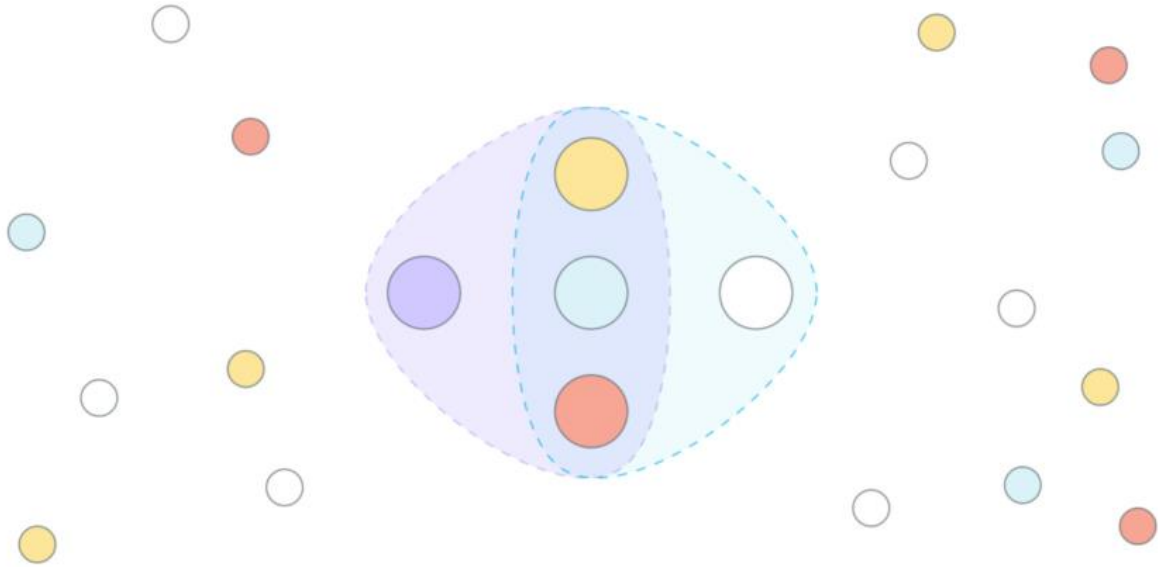
SCP – jak rozproszona sieć Stellar dochodzi do zgody

Stellar (XLM) to nie tylko kryptowaluta, lecz również rozproszona infrastruktura rozliczeniowa, której przyświeca idea, że świat potrzebuje tanich, szybkich i niezawodnych transakcji oraz nowego, otwartego systemu rozliczeniowego. Kolejnym z fundamentów Stellar jest możliwość dokonywania transakcji bez względu na fizyczne granice, łącząc tym samym ludzi z różnych zakątków świata (nie sposób zauważyć, że wszystkie z kryptowalut to umożliwiają). Zajmuje on zaszczytne miejsce w TOP 10 kryptowalut pod względem kapitalizacji.

SCP[4] (Stellar Consensus Protocol) jest narzędziem, dzięki któremu rozproszone na cały świat węzły sieci Stellar mogą dojść między sobą do porozumienia w sprawie aktualnego stanu sieci. Inaczej niż w standardowym systemie bankowym, kiedy to istnieje jedna centralna baza danych, kryptowaluty wymagają osiągania zgody pomiędzy wieloma, niezależnymi węzłami autoryzującymi wszystkie transakcje w sieci. Co więcej, muszą być w stanie zrobić to, nawet w przypadku kiedy część z węzłów okaże się niesprawna lub wadliwa, zaatakowana. Stellar posiada aktualnie 64[5] węzły walidujące wszystkie transakcje odbywające się w ramach jego blockchainu. SCP bazuje, pod względem fundamentalnym, na założeniach znanych z protokołu BFT, który czyni zdecentralizowany system odporny na błędy wynikające z problemu Generałów Bizantyjskich.

BFT (Bizantine Fault Tolerance) to protokół za pomocą którego, pomimo pojawiania się nieuczciwych węzłów, znanych z problemu o Generałach Bizantyjskich[6], dochodzi do zawarcia porozumienia w określonej, zdecentralizowanej sieci. BFT ustanawia konsensus i tzw. odporność na błędy bizantyjskie (są to po prostu rodzaje błędów wynikające z Problemu Generałów Bizantyjskich – np. co zrobić, jeśli jeden z generałów okaże się zdrajcą? – przekładając to na sieci komputerowe – jak zdecentralizowana sieć ma dojść do porozumienia, w momencie którym jeden z węzłów głównych nie jest godny zaufania.) W BFT węzły nieustannie wysyłają do siebie „wiadomości" dzięki którym pozostają w porozumieniu. BFT potrzebuje minimum 66.(6)% uczciwych węzłów do osiągnięcia konsensusu. Co ciekawe węzły w BFT muszą być również niezwykle precyzyjnie zgrane w czasie (posiadać te same znaczniki czasowe), najmniejsze opóźnienia mogą prowadzić do krytycznych błędów sieci.

[4] https://www.stellar.org/papers/stellar-consensus-protocol.pdf
[5] https://stellarbeat.io/
[6] Wikipedia: Problem Generałów Bizantyjskich



Rysunek 1: Model Federacyjnego porozumienia bizantyjskiego

FBA[7] wykorzystywany w Stellar jest uogólnieniem porozumienia bizantyjskiego (BA). Jeśli wszystkie z węzłów zdecydują się utworzyć takie samo kworum zaufanych węzłów, FBA staje się po prostu BA. Czym zatem jest kworum i jak dokładnie działa Stellar?

Węzły w sieci Stellar wykorzystują unikatowy mechanizm wymyślony przez twórców Stellar, a nazywany FBA (Federated Bizantine Agreement). Węzły, zamiast w każdym momencie w czasie łączyć się ze wszystkimi pozostałymi węzłami, w celu dojścia do prawidłowego porozumienia tworzą kworum.

W prostych słowach FBA zakłada:

- Węzły wybierają grupę węzłów którym ufają i nie obchodzi ich reszta
- Węzły tworzą grupy w obrębie których dochodzi do porozumienia odnośnie transakcji
- Jak tylko konsensus zajdzie w lokalnych grupach, porozumiewają się one ze sobą i dochodzi do zgody w całej sieci
- Panuje asymetryczna struktura ważności węzłów (patrz Rysunek 3)[8]
- Każdy może dołączyć do sieci i stać się węzłem (obecny koszt utrzymania takiego węzła to ok. 40$ miesięcznie)

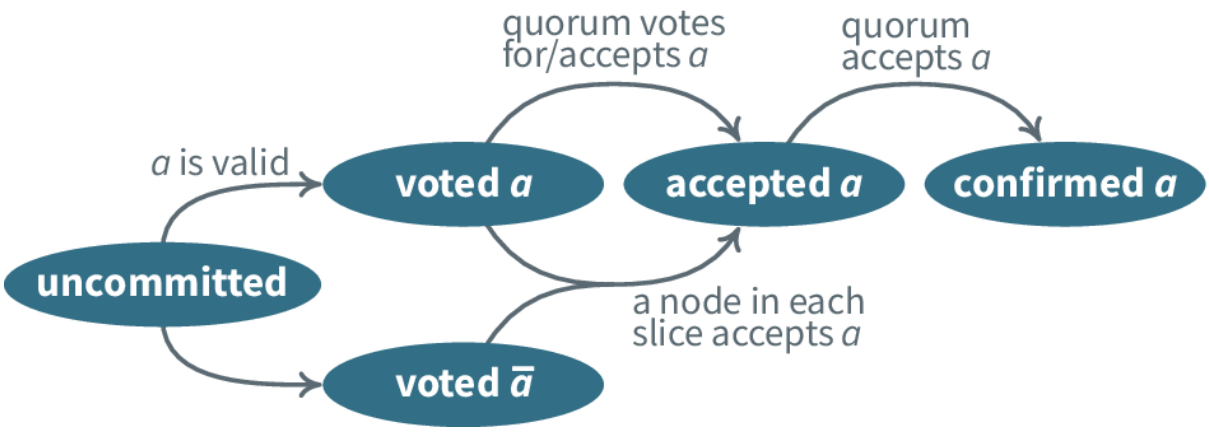
[7] https://www.youtube.com/watch?v=X3Gj2nQZCNM
[8] http://muratbuffalo.blogspot.com/2018/04/the-stellar-consensus-protocol.html

Federacyjna wersja porozumienia bizantyjskiego zastosowana w SCP (Stellar Consensus Protocol) wprowadza do modelu konsensusu sieciowego dwa ważne mechanizmy:

A) Głosowanie federalne
B) Federalna elekcja liderów pośród węzłów

Głosowanie federalne polega na tym, że każdy z węzłów biorący w nim udział, może wysłać potwierdzenie lub zaprzeczenie do wystosowanego przez inny węzeł stwierdzenia: „transakcja x została wprowadzona w sieć Stellar i powinna zostać zatwierdzona w głównym łańcuchu". Jeżeli głosowanie pomiędzy kworum zaufanych węzłów okaże się sukcesem i żaden z węzłów nie odrzuci transakcji jako nieprawidłowej, zostaje ona przyjęta do sieci. Głosowanie federalne odbywa się wewnątrz kworum zaufanych węzłów, jednocześnie dynamicznie ustalając granicę określonego kworum.

Głosowanie federalne odbywa się w trzech fazach. W fazie pierwszej węzły nadają transakcję, następnie jest ona akceptowana, na samym końcu zaś zatwierdzana i przekazywana do głównego łańcucha.



Rysunek 2: Proces głosowania federalnego w Stellar

Podczas federalnej elekcji wszystkie węzły w sieci Stellar decydują, które z węzłów posiadać powinny najwyższą ważność w kwestii ustalania porozumienia. Głosowanie ma charakter pseudolosowy[9].

Federalna elekcja pozwala każdemu z węzłów wybrać lidera, w taki sposób, aby w danym kworum był jeden lider, lub bardzo mała ich ilość. Dodatkowo sieć zabezpieczona jest przed dokonaniem wyboru błędnego lidera – w tym celu stosowany jest mechanizm rund. Jeśli

[9] http://www.scs.stanford.edu/~dm/blog/simplified-scp.html

przywódcy obecnej rundy wydają się nie wypełniać swoich obowiązków, po pewnym okresie węzły przechodzą do następnej rundy, aby rozwinąć grupę przywódców, których śledzą. W taki sposób, w danym kworum zaufanych węzłów, może zostać wybrany jeden bądź więcej liderów.

Kwestie bezpieczeństwa w protokole FBA

FBA cechuje się asymetryczną architekturą – różne węzły mają różną wartość, dlatego nawet w przypadku ataku typu Sybil[10], atakujący mogą utworzyć pełne kworum składające się z błędnie funkcjonujących i wadliwych węzłów, a mimo to nie wpłynął one na złamanie konsensusu w sieci Stellar. Pojawia się jednak pytanie, czy w zdecentralizowanej kryptowalucie wszystkie pełne węzły nie powinny być równe?

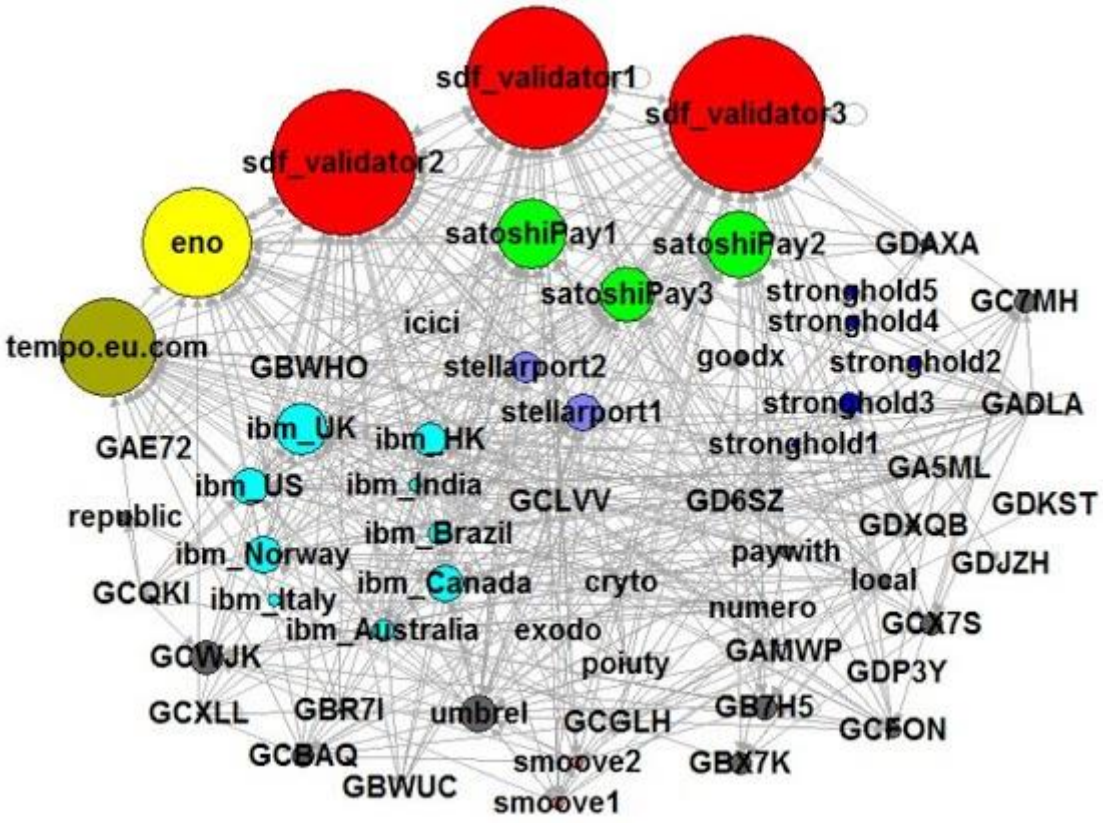
FBA preferuje bezpieczeństwo sieci i to, że węzły pozostaną w zgodzie, nad żywotność i ewentualne opóźnienia w transakcjach (lepiej, aby transakcje były opóźnione, aniżeli doszło do niezgody pośród węzłów, która mogłaby prowadzić do podwójnego wydatkowania tych samych środków – ang. double spending). FBA więc, poniekąd gwarantuje, że w przypadku utraty zgody w sieci, nie dojdzie do forku, czyli rozłamania głównego łańcucha na dwa różne.

Dodawanie lub usuwanie węzłów w przypadku błędu sieci wymaga dojścia do porozumienia (konsensusu) między pozostałymi węzłami. W zamkniętym systemie nie jesteśmy w stanie tego zrobić, kiedy protokół „obsługujący" porozumienie w sieci jest dosłownie martwy. FBA natomiast, o ile nie dojdzie do krytycznego błędu oprogramowania który trzeba naprawić przed wznowieniem działania blockchainu, pozwala węzłom tak dopasować kworum, aby możliwe było automatyczne przywrócenie sieci do prawidłowego funkcjonowania.

Wiecie już jak węzły sieci Stellar dochodzą między sobą do porozumienia. Czas więc przyjrzeć się dlaczego aktualna konfiguracja FBA wykorzystywana przez Stellar jest silnie scentralizowana i możliwe jest zaatakowanie całej sieci, skupiając się jedynie na trzech z głównych węzłów, posiadanych przez Fundację Stellar.

Wyniki badań zespołu z KAIST – Stellar jest silnie scentralizowany

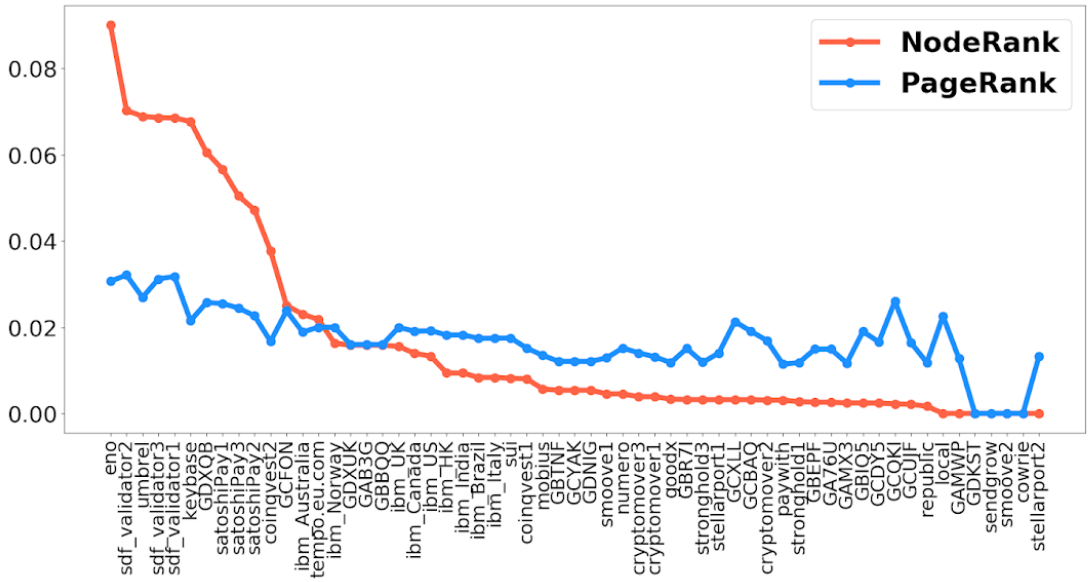
[10] https://www.binance.vision/pl/security/sybil-attacks-explained



Rysunek 3: Wizualizacja poszczególnych kworum w sieci Stellar

Rysunek przedstawia strukturę wycinków kworum w dniu 22 stycznia 2019 r. Każdy okrąg reprezentuje jeden węzeł walidujący. Rozmiar okręgu jest proporcjonalny do liczby przypadków, w których węzeł jest zawarty w dowolnym wycinku kworum. Wierzchołki o tym samym kolorze są prowadzone przez tę samą organizację.

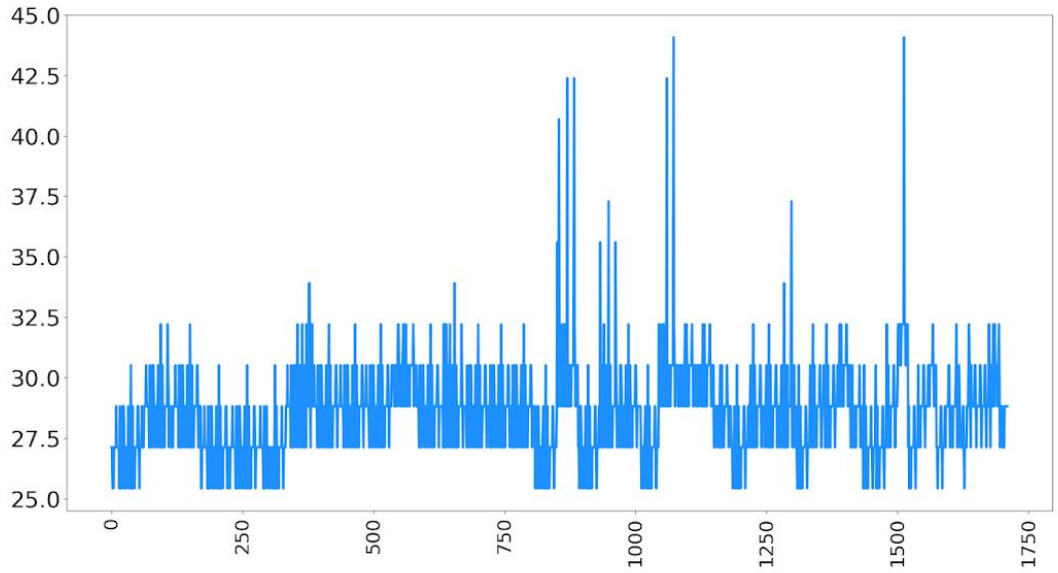
Można jasno zauważyć, że węzły podpisane jako sdf_validator są najczęściej uwzględniane w dochodzeniu do zgody w obrębach kworum – najwięcej z węzłów ma oznaczone je jako zaufane. Warto zaznaczyć, że cała trójka z tych węzłów należy do Stellar Development Foundation.



Rysunek 4: Waga węzłów w sieci Stellar

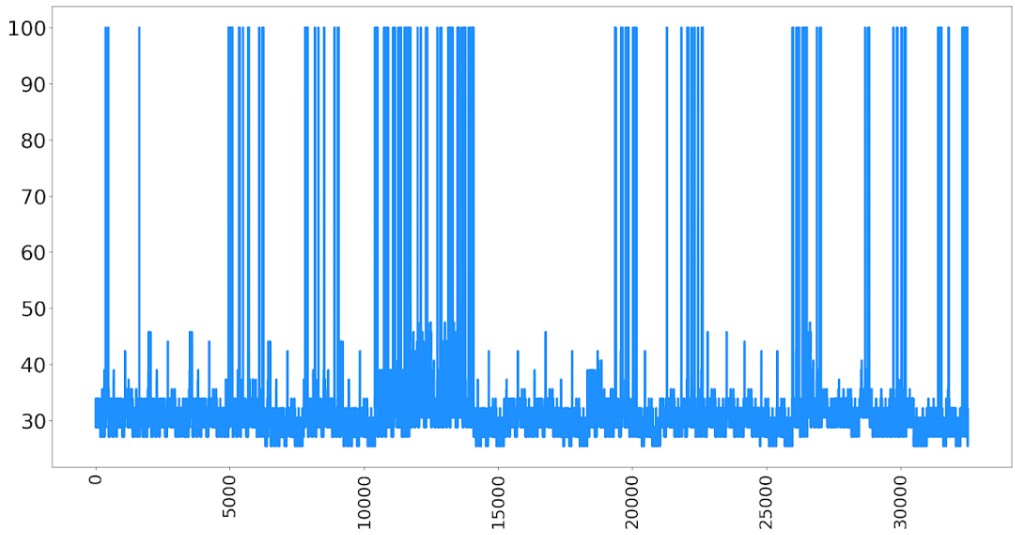
Na powyższej wizualizacji możecie natomiast zobaczyć, jaką wagę odgrywają w dochodzeniu do konsensusu poszczególne węzły w sieci Stellar. Są to zaktualizowane dane z 1.05.2019 r.

Posiadając te dane, przyjrzymy się więc, jak zablokować sieć Stellar.



Rysunek 5: 2 z największych węzłów zostają zaatakowane

Jak możemy zauważyć, w przypadku ataku na dwa z trzech największych węzłów zarządzanych przez Fundację Stellar, sieć staje się niesprawna w 42.5%.

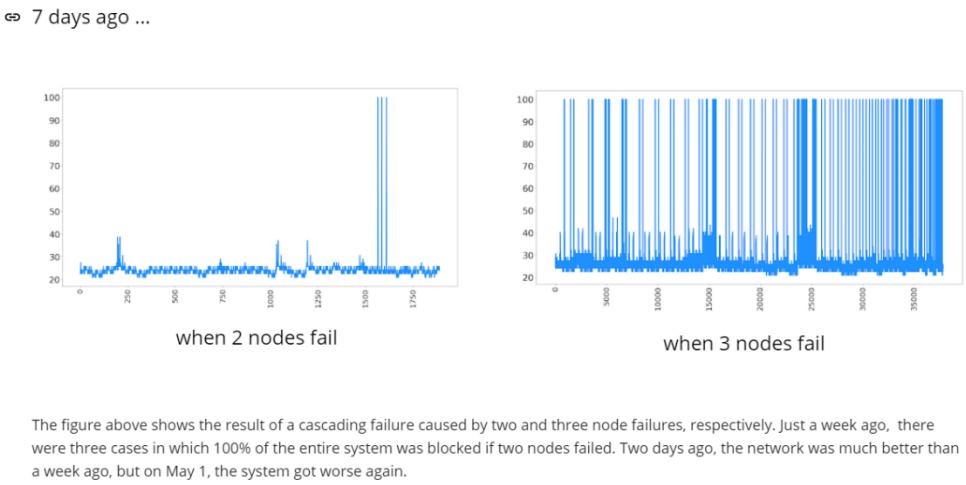


Rysunek 6: Atak na 3 z największych węzłów

Powyższa wizualizacja przedstawia natomiast skutki ataku na trzy z największych węzłów uczestniczących w globalny konsensusie sieci Stellar. W każdym przypadku, jeżeli trzy z największych węzłów zostaną skutecznie zaatakowane, cały blockchain Stellar przestaje funkcjonować.

Przy aktualnej topologii FBA którą wykorzystuje Stellar, blockchain ten jest silnie scentralizowany i podatny na awarie w przypadku ataku na te trzy konkretne węzły, zarządzane przez jedną organizację.

Błędem byłoby zakładanie, że takie zagrożenie istnieje tylko w sferze symulacji i badań. Jest ono jak najbardziej realne, co pokazują dane historyczne z ostatnich 7 dni. Obrazują one możliwość wyłączenia sieci w przypadku ataku na 2 lub 3 główne węzły:



Rysunek 7: Stellar - dane historyczne

Wniosek:

Jeżeli Stellar Development Foundation nie zmieni modelów kworum na bardziej zdecentralizowany, sieć Stellar dalej będzie podatna na tego typu ataki.

Ostatnią interesującą rzeczą jaką chciałbym przedstawić jest niski współczynnik tzw. „niezależnych" walidatorów. Czyli uczestników sieci/węzłów, nie mających bezpośredniej inicjatywy finansowej ze współpracy z Stellar:

Table I
MOTIVATIONS OF PLAYERS PARTICIPATING IN STELLAR AS VALIDATORS.

Purpose	Type	Number of players	Rate (%)
For-profit	Business with Stellar	23	74.2
	Stellar Foundation	3	9.7
Non-profit	Individual	1	3.2
Unknown		4	12.9

Rysunek 8: Węzły związane/niezwiązane biznesowo ze Stellar

W interesie każdej kryptowaluty pragnącej uzyskać decentralizację, a przez to zwiększyć swoją odporność na błędy wynikające z np. ataku sieci, jest zwiększanie liczby niezależnych uczestników sieci posiadających węzły uczestniczące w globalnym konsensusie. Na chwilę obecną, 83.9% węzłów związana jest biznesowo ze Stellar, 3.2% stanowi węzły funkcjonujące na zasadzie non-profit, a 12.9% jest nieznane.

Podsumowanie

Analiza wykazała, że obecne ułożenie kworum w systemie Stellar jest silnie scentralizowane, przez co podatne na realne ataki (czego dowodzą dane historyczne). Po opublikowaniu badania, Stellar Development Foundation zaczęło podejmować kroki w celu zmiany tego stanu rzeczy. Na razie jednak, sieć pozostaje tak samo podatna na zagrożenia jak w momencie przeprowadzenia badań.

Kryptowaluty, wraz z ich gwałtownym rozwojem stają się coraz bardziej skomplikowane. Fundamentalne protokoły dochodzenia do konsensusu w obrębie zdcentralizowanej sieci stanowią poważne wyzwanie dla deweloperów z całego świata. Na chwilę obecną, liczne badania sugerują, że istnieje poważny problem ze skalowaniem systemu, w szczególności prędkości transakcji na sekundę i przepustowości sieci, jednocześnie pozostawiając system odpowiednio zdecentralizowanym i obniżając podatność na ataki ze strony nieuczciwych uczestników.

stokarz