УДК 338

ОЦЕНКА НАДЕЖНОСТИ И РЕГРЕССИОННЫЙ АНАЛИЗ ЗАКРЫТИЯ СДЕЛОК ПО ОПЕРАЦИЯМ С БИТКОЙНОМ

Фредерик Аннинг

Студент международной магистерской программы «Banking»

Сибирский федеральный университет

Красноярск, Россия

Аннотация

В данной статье оценивается позиция рискового инвестора посредством операционных обменов биткойнов, конвертирующего биткойны в твердую валюту. Мы рассматриваем причину совершения этих сделок, направления вложений инвесторов, а также направления инвестирования в обмен валют.

Ключевые слова: биткойны, инвесторы, биржа.

AN ASSESSMENT OF THE SURVIVAL& REGRESSION ANALYSIS OF EXCHANGE CLOSURES IN BITCOIN OPERATIONS

Frederick Anning

Graduate Student

Siberian Federal University

School of Economics Management & Environmental Studies

Krasnoyarsk, Russia

Abstract

We by this paper assess the risk investor’s face by way of operating Bitcoin exchanges, which however convert Bitcoins into hard currency. We examine the cause of closure of these exchanges and what investors should look for as well as the path to take in investing in an exchange.

Keywords: Bitcoins, Investors, Exchange

Introduction

Employing a survival as well as a regression analysis of Bitcoin exchanges has shown that there is an inverse correlation regarding the probability of an exchange closure in terms of its trade sizes; we also by an analysis regarding a logistic regression is able to indicate that popular exchanges are more prone to suffer security breaches. This article however does an assessment using the indicated modules.

Methodology

Survival analysis is a way in estimating the time taken for a Bitcoin exchange to close as well as a way in identifying the factors that could trigger the closure.
Vigorous assessment entails bearing in mind the fact that some exchanges continue to open even at the end of measuring the interval (taking out data points).
We however begin by taking into account two mathematical functions i.e.;

- Survival functions; denoted by **S (t) -** however measures the probability that there will be continuous exchange in operation for beyond **t** days.
- Hazard function; denoted by **h (t)** – also however measures the instantaneous and or immediate risk of closure at a time period **t**.

In identifying the factors that affect the time for an exchange's survival, we however employ the Cox proportional hazards model instead of the linear regression model; the survival function could also be estimated by employing the best-fit Cox model [1].

Deducing a statistical model

We begin by postulating that the survival time of a bitcoin exchange is affected by three variables;

- The average daily transaction volume: - profitability is a major factor of concern; i.e. an exchange can only operate if it is profitable; this however generally involves realizing scale in the quantity of payment generated transactions accomplished in terms of fees [2]. It is however expected that exchanges with low deal sizes are more probable to be closed. We however employ a log-transformation of the deals sizes taking into account how skewed the size of the deals are.
- Realizing a security breach: in the event there is a breach in security profits could be eroded, there could also be a reduction in cash flow, and existing and or prospective customers could be scared off [3]. When we realized same there is the expectation that breached exchanges be closed.
- Compliance with AML/CFT: there is a general concern by some Bitcoin exchanges that they are being pressurized by policy makers and regulators within the finance industry and such exchanges operating within countries with more focus on anti-money laundering concerns could be pressured with legislations and policies thus making them close operations.

We can however deduce a corresponding model for proportional hazards as [1]:

$$\boldsymbol{h_i(t) = h_0(t)\exp(\beta_1 \log(Daily\ vol.)_i + \beta_2 Breached_i + \beta_3 AML_i}$$

We however define the variables as, $\mathbf{h_i(t)}$ being the hazard rate for exchange ***i, log (Daily vol.)***$_i$ the transaction volume at exchange ***i, Breached***$_i$ designates whether or not exchange ***i*** suffered a breach in security, whereas $\boldsymbol{AML_i}$ represents the **AML/CFT** compliance score for the country where the exchange is incorporated. $\boldsymbol{_1; _2; _3}$ are however the best-fit constants, where aas $\boldsymbol{h_0(t)}$ is however the unspecified hazard on the baseline.

Research has shown that the daily volume generated is associated negatively with the rate of hazard: when the daily volumes are doubled the daily volume rate matches to a reduction in the rate of hazard [4]. This is to say the probability of closing an exchange is dependent on the number of transactions processed by the exchange and as such an exchange which process more transactions is less probable to close down.

Realizing a problem regarding breaches is positively correlated with hazard, however, the correlation will fall short of being statistically significant at a given time period. With a record of just nine exchanges which has publicly reported problems regarding breaches and only five of these exchanges closed, it is however of no surprise that the association is currently not solid in its footing.

It is also noteworthy that the anti-money laundering index has no bearing with regards to measuring correlation with instances where exchanges may be closed; and as such an oversight in regulations does not trigger closure of an exchange, that notwithstanding it could also reflect that the indicator however does not necessarily convey accurately the differences regarding attitudes which regulators and or policy makers within the world's financial industries have regarding the operation and or trading in Bitcoins.

Employing the best-fit survival function with regards to the Cox model [1]; the survival function accurately computes the probability of failure within a given time period. Bitcoin investors are able to assess their risk position before investing in an exchange.

Regression Analysis of Exchange Breaches

Though we cannot not specifically say that security breaches trigger close down of exchanges we can however examine whether or not any other factors are likely going to affect an exchange may suffer breaches.

Deducing a Statistical Model

We further employ the model for logistic regression with a dependent variable signifying whether or not an exchange experiences a breach [5]. We again postulate that two descriptive variables have an impact on whether or not a breach will occur. Per our postulation we consider the;

- The average daily size of transactions: in the event of bigger exchanges our targets becomes richer. This stems from the fact that as an exchange processes more transactions there is an increase in the flow of wealth into the accounts. Therefore, the expectation is that criminals with profit-motivated intents are naturally drawn to exchanges which have higher average daily deals in terms of size [6].
- Monthly operational size: The daily operation of an exchange poses a lot of threats since that day tends to be a that day of a possible hack into the system. Exchanges that operate for long are however prone to breaches;

Our deduced model then shows as below;

$$\boldsymbol{log(p_b/(1-p_b)) = c_0 + (c_1 \log(Daily\ \ vol.) + c_2 months\ operational + \varepsilon.}$$

Our dependent variable p_b is thus the probability that an exchange may experience a breach in security, c_0; c_1; c_2 are however our best-fit constants, the log (daily vol.) is our log-transformed daily deal size at the exchange, our months operational is the time (in months) that an exchange is operational, and " it is however an error term.

Conclusion

It is also worthy to note that the size of a transaction is positively correlated with experiencing breaches. The Months operational on the other hand is negatively correlated with breaches, but its association falls short of statistical significance. In view of this we are faced with a puzzle, i.e. high sizes in terms of exchanges are less likely to close on one hand, and on the other hand are more likely to experience breaches. Now investors of Bitcoin can however choose to transact business with less popular exchanges thus reducing their risk of losing money because of a breach, or transacting business with more popular exchanges that may possibly be breached on one hand, but on the other hand are less likely to shut down without prior notice.

References

1. Cox, D.: Regression models and life-tables. Journal of the Royal Statistics Society, Series B 34 (1972) 187–220
2. Bohme et al (2015)., Bitcoin: Economics, Technology an governance
3. Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better – how to make Bitcoin a better currency. In: Proc. Financial Crypto, Bonaire, N.A. (February 2012)
4. Karame, G., Androulaki, E., Capkun, S.: Two Bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin. In: Proc. ACM CCS, Raleigh, NC (October 2012)
5. Ron, D., Shamir, A.: Quantitative analysis of the full Bitcoin transaction graph (October 2012) Cryptology ePrint Archive, Report 2012/584.
6. Reid, F., Harrigan, M.: An analysis of anonymity in the Bitcoin system (May 2012) arXiv:1107.452a4v2 [physics.soc-ph]. http://arxiv.org/abs/1107.4524.