Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk

Tyler Moore[1] and Nicolas Christin[2]

[1] Computer Science & Engineering, Southern Methodist University, USA
tylerm@smu.edu
[2] INI & CyLab, Carnegie Mellon University, USA
nicolasc@cmu.edu

Abstract. Bitcoin has enjoyed wider adoption than any previous cryptocurrency; yet its success has also attracted the attention of fraudsters who have taken advantage of operational insecurity and transaction irreversibility. We study the risk investors face from Bitcoin exchanges, which convert between Bitcoins and hard currency. We examine the track record of 40 Bitcoin exchanges established over the past three years, and find that 18 have since closed, with customer account balances often wiped out. Fraudsters are sometimes to blame, but not always. Using a proportional hazards model, we find that an exchange's transaction volume indicates whether or not it is likely to close. Less popular exchanges are more likely to be shut than popular ones. We also present a logistic regression showing that popular exchanges are more likely to suffer a security breach.

Keywords: Bitcoin, currency exchanges, security economics, cybercrime.

1 Introduction

Despite added benefits such as enhanced revenue [1] or anonymity [2], and often elegant designs, digital currencies have until recently failed to gain widespread adoption. As such, the success of Bitcoin [3] came as a surprise. Bitcoin's key comparative advantages over existing currencies lie in its entirely decentralized nature and in the use of proof-of-work mechanisms to constrain the money supply. Bitcoin also benefited from strongly negative reactions against the banking system, following the 2008 financial crisis: Similar in spirit to hard commodities such as gold, Bitcoin offers an alternative to those who fear that "quantitative easing" policies might trigger runaway inflation.

As of January 2013, Bitcoin's market capitalization is approximately US$187 million [4]. However, with success comes scrutiny, and Bitcoin has been repeatedly targeted by fraudsters. For instance, over 43,000 Bitcoins were stolen from the Bitcoinica trading platform in March 2012 [5]; in September 2012, $250,000 worth of Bitcoins were pilfered from the Bitfloor currency exchange [6]. Interestingly, experience from previous breaches does not suggest that failures necessarily trigger an exodus from the currency. In fact, with two possible exceptions—a June 2011 hack into the largest Bitcoin currency exchange, which coincided with the USD-Bitcoin exchange rate peaking, and the August 2012 downfall of the largest Bitcoin Ponzi scheme [8]—the (volatile) Bitcoin exchange rate has fluctuated independently from disclosed hacks and scams.

A.-R. Sadeghi (Ed.): FC 2013, LNCS 7859, pp. 25–33, 2013.

While Bitcoin's design principles espouse decentralization, an extensive ecosystem of third-party intermediaries supporting Bitcoin transactions has emerged. Intermediaries include currency exchanges used to convert between hard currency and Bitcoin; marketplace escrow services [7]; online wallets; mixing services; mining pools; or even investment services, be they legitimate or Ponzi schemes [8]. Ironically, most of the risk Bitcoin holders face stems from interacting with these intermediaries, which operate as de facto centralized authorities. For instance, one Bitcoin feature prone to abuse is that transactions are irrevocable, unlike most payment mechanisms such as credit cards and electronic fund transfers. Fraudsters prefer irrevocable payments, since victims usually only identify fraud after transactions take place [9, 10]. Irrevocability makes any Bitcoin transaction involving one or more intermediaries subject to added risk, such as if the intermediary becomes insolvent or absconds with customer deposits.

In this paper, we focus on one type of intermediary, currency exchanges, and empirically examine the risk Bitcoin holders face from exchange failures. Section 2 explains our data collection and measurement methodology. Section 3 presents a survival analysis of Bitcoin exchanges, and shows that an exchange probability of closure is inversely correlated to its trade volumes. Section 4 complements this analysis with a logistic regression that indicates that popular exchanges are more likely to suffer security breaches. Section 5 reviews related work and Section 6 discusses follow-up research.

2 Data on Bitcoin-Exchange Closures

2.1 Data Collection Methodology

We begin by collecting historical data on the Bitcoin exchange rates maintained by the website `bitcoincharts.com`. This includes the daily trade volumes and average weighted daily price for 40 Bitcoin exchanges converting into 33 currencies until January 16, 2013, when the data collection was made. We calculated the average daily trade volume for each exchange by tallying the total number of Bitcoins converted into all currencies handled by the exchange for the days the exchange was operational.

We also calculate the "lifetime" of each exchange, that is, the number of days the exchange is operational, denoted by the difference between the first and last observed trade. We deem an exchange to have closed if it had not made a trade in at least two weeks before the end of data collection. We further inspected the existence of a report on the Bitcoin Wiki [11] or on Bitcoin forums [12] to confirm closure, and determine whether closure was caused by a security breach (e.g., hack or fraud). We also checked for reports on whether or not investors were repaid following the exchange's closure.

Finally, to assess regulatory impact, we attempted to identify the country where each exchange is based. We then used an index (ranging between 0 and 49) computed by World Bank economists [13] to identify each country's compliance with "Anti-Money-Laundering and Combating the Financing of Terrorism" (AML-CFT) regulations [13].

2.2 Summary Statistics

Table 1 lists all 40 known Bitcoin currency exchanges, along with relevant facts about whether the exchange later closed. Nine exchanges experienced security breaches,

Table 1. Bitcoin exchange indicators. "Origin" denotes the jurisdiction under which the exchange operates, "AML," the extent to which the exchange's jurisdiction has implemented "Anti-Money Laundering and Combating the Financing of Terrorism" international standards [13]. "Risk ratio" is the relative risk of exchange failure based on the Cox proportional hazards model (Section 3).

Exchange	Origin	Dates Active	Daily vol.	Closed?	Breached?	Repaid?	AML	Risk Ratio
BitcoinMarket	US	4/10 – 6/11	2454	yes	yes	–	34.3	1.12
Bitomat	PL	4/11 – 8/11	758	yes	yes	yes	21.7	1.28
FreshBTC	PL	8/11 – 9/11	3	yes	no	–	21.7	2.01
Bitcoin7	US/BG	6/11 – 10/11	528	yes	yes	no	33.3	1.59
ExchangeBitCoins.com	US	6/11 – 10/11	551	yes	no	–	34.3	0.65
Bitchange.pl	PL	8/11 – 10/11	380	yes	no	–	21.7	0.61
Brasil Bitcoin Market	BR	9/11 – 11/11	0	yes	no	–	24.3	3.85
Aqoin	ES	9/11 – 11/11	11	yes	no	–	30.7	1.57
Global Bitcoin Exchange	?	9/11 – 1/12	14	yes	no	–	27.9	1.45
Bitcoin2Cash	US	4/11 - 1/12	18	yes	no	–	34.3	1.47
TradeHill	US	6/11 - 2/12	5082	yes	yes	yes	34.3	0.94
World Bitcoin Exchange	AU	8/11 – 2/12	220	yes	yes	no	25.7	1.80
Ruxum	US	6/11 – 4/12	37	yes	no	yes	34.3	1.24
btctree	US/CN	5/12 – 7/12	75	yes	no	yes	29.2	0.98
btcex.com	RU	9/10 – 7/12	528	yes	no	no	27.7	0.61
IMCEX.com	SC	7/11 – 10/12	2	yes	no	–	11.9	1.88
Crypto X Change	AU	11/11 – 11/12	874	yes	no	–	25.7	0.53
Bitmarket.eu	PL	4/11 – 12/12	33	yes	no	no	21.7	1.09
bitNZ	NZ	9/11 – pres.	27	no	no	–	21.3	1.14
ICBIT Stock Exchange	SE	3/12 – pres.	3	no	no	–	27.0	2.15
WeExchange	US/AU	10/11 – pres.	2	no	no	–	30.0	2.23
Vircurex	US?	12/11 – pres.	6	no	yes	–	27.9	4.41
btc-e.com	BG	8/11 – pres.	2604	no	yes	yes	32.3	1.08
Mercado Bitcoin	BR	7/11 – pres.	67	no	no	–	24.3	0.95
Canadian Virtual Exchange	CA	6/11 – pres.	832	no	no	–	25.0	0.53
btcchina.com	CN	6/11 – pres.	473	no	no	–	24.0	0.60
bitcoin-24.com	DE	5/12 – pres.	924	no	no	–	26.0	0.52
VirWox	DE	4/11 – pres.	1668	no	no	–	26.0	0.45
Bitcoin.de	DE	8/11 – pres.	1204	no	no	–	26.0	0.49
Bitcoin Central	FR	1/11 – pres.	118	no	no	–	31.7	0.91
Mt. Gox	JP	7/10 – pres.	43230	no	yes	yes	22.7	0.49
Bitcurex	PL	7/12 – pres.	157	no	no	–	21.7	0.76
Kapiton	SE	4/12 – pres.	160	no	no	–	27.0	0.80
bitstamp	SL	9/11 – pres.	1274	no	no	–	35.3	0.54
InterSango	UK	7/11 – pres.	2741	no	no	–	35.3	0.45
Bitfloor	US	5/12 – pres.	816	no	yes	no	34.3	1.45
Camp BX	US	7/11 – pres.	622	no	no	–	34.3	0.63
The Rock Trading Company	US	6/11 – pres.	52	no	no	–	34.3	1.14
bitme	US	7/12 – pres.	77	no	no	–	34.3	1.04
FYB-SG	SG	1/13 – pres.	3	no	no	–	33.7	2.23

caused either by hackers or other criminal activity. Five of these exchanges subsequently closed, but four have survived so far (Mt. Gox, `btc-e.com`, Bitfloor, and Vircurex). Another 13 closed without experiencing a publicly-announced breach.

The popularity of exchanges varied greatly, with 25% of exchanges processing under 25 Bitcoins each day on average, while the most popular exchange, Mt. Gox, has averaged daily transactions exceeding 40 000 BTC. The median daily transactions carried out by exchanges is 290, while the mean is 1 716.

One key factor affecting the risk posed by exchanges is whether or not its customers are reimbursed following closure. We must usually rely on claims by the operator and investors if they are made public. Of the 18 exchanges that closed, we have found evidence on whether customers were reimbursed in 11 cases. Five exchanges have not

reimbursed affected customers, while six claim to have done so. Thus, the risk of losing funds stored at exchanges is real but uncertain.

As a first approximation, the failure rate of Bitcoin exchanges is 45%. The median lifetime of exchanges is 381 days. These summary statistics obscure two key facts: exchanges are opened at different times and so their maximum potential lifetimes vary, and a majority of exchanges remain viable at the end of our observation period. Survival analysis can properly account for this.

3 Survival Analysis of Exchange Closure

We use survival analysis to estimate the time it takes for Bitcoin exchanges to close and to identify factors that can trigger or stave off closure. Robust estimation requires considering that some exchanges remain open at the end of our measurement interval ("censored" data points). Two mathematical functions are commonly used. First, a survival function $S(t)$ measures the probability that an exchange will continue to operate longer than for t days. Second, a hazard function $h(t)$ measures the instantaneous risk of closure at time t. To identify factors affecting an exchange's survival time, we use a Cox proportional hazards model [14], rather than traditional linear regression. We can also estimate the survival function using the best-fit Cox model.

3.1 Statistical Model

We hypothesize that three variables affect the survival time of a Bitcoin exchange:

Average daily transaction volume: an exchange can only continue to operate if it is profitable, and profitability usually requires achieving scale in the number of fee-generating transactions performed. We expect that exchanges with low transaction volume are more likely to shut down. We use a log-transformation of the transaction volume given how skewed transaction volumes are.

Experiencing a security breach: suffering a security breach can erase profits, reduce cash flow, and scare away existing and prospective customers. We thus expect breached exchanges to be more likely to subsequently close.

AML/CFT compliance: some Bitcoin exchanges complain of being hassled by financial regulators. Thus, exchanges operating in countries with greater emphasis on anti-money laundering efforts may be pressured into shutting down.

We then construct a corresponding proportional hazards model [14]:

$$h_i(t) = h_0(t) \exp(\beta_1 \log(\text{Daily vol.})_i + \beta_2 \text{Breached}_i + \beta_3 \text{AML}_i).$$

Here, $h_i(t)$ is the hazard rate for exchange i, $\log(\text{Daily vol.})_i$ is the transaction volume at exchange i, Breached_i indicates whether exchange i suffered a security breach, and AML_i denotes the AML/CFT compliance score for the exchange's country of incorporation. $\beta_1, \beta_2, \beta_3$ are best-fit constants, and $h_0(t)$ is the unspecified baseline hazard.

3.2 Results

The best-fit Cox model is:

		coef.	exp(coef.)	Std. Err.	Significance
$\log(\text{Daily vol.})_i$	β_1	-0.173	0.840	0.072	$p = 0.0156$
Breached_i	β_2	0.857	2.36	0.572	$p = 0.1338$
AML_i	β_3	0.004	1.004	0.042	$p = 0.9221$
log-rank test: Q=7.01 ($p = 0.0715$), $R^2 = 0.145$					

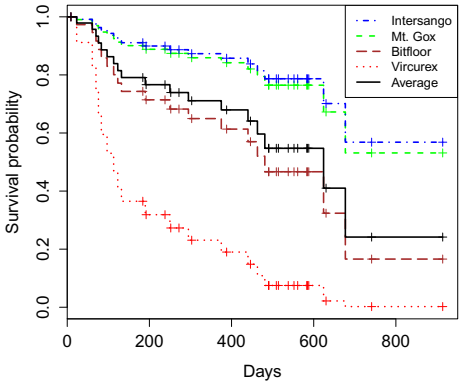

Fig. 1. Empirically-derived survival probability function for Bitcoin exchanges

The daily volume is negatively associated with the hazard rate ($\beta_1 = -0.173$): doubling the daily volume rate corresponds to a 16% reduction in the hazard rate ($\exp(\beta_1) = 0.84$) . Thus, exchanges that process more transactions are less likely to shut down.

Suffering a breach is positively correlated with hazard, but with a p-value of 0.1338, this correlation falls just short of being statistically significant at this time. Given that just nine exchanges publicly reported suffering breaches and only five later closed, it is not surprising that the association is not yet robust.

Finally, the anti-money laundering indicator has no measurable correlation with exchange closure. This could suggest that regulatory oversight is not triggering closures, but it could also reflect that the indicator itself does not accurately convey differences in attitudes the world's financial regulators have taken towards Bitcoin.

Figure 1 plots the best-fit survival function according to the Cox model. The survival function precisely quantifies the probability of failure within a given amount of time. This can help Bitcoin investors weigh their risks before putting money into an exchange-managed account. The black solid line plots the estimated survival function for the best fit parameters outlined above for the mean values of exchange volume,

whether a site has been hacked, and AML score. For instance, $S(365) = 0.711$ with 95% confidence interval $(0.576, 0.878)$: there is a 29.9% chance a new Bitcoin exchange will close within a year of opening (12.2%–42.4% with 95% confidence).

Figure 1 also includes survival functions for several Bitcoin exchanges. These are calculated based on the exchange's values for parameters in the Cox model (e.g., transaction volume). For instance, Mt. Gox and Intersango are less likely to close than other exchanges. Meanwhile, Vircurex (established in December 2011 and breached in January 2013) continues to operate despite low transaction volumes and a survival function that estimates one-year survival at only 20%.

The right-most column in Table 1 presents relative risk ratios for all exchanges. These indicate how the hazard function for each exchange compares to the baseline hazard. Values less than 1 indicate that the exchange is at below-average risk for closure; values greater than 1 denote above-average risk. Of course, any exchange may close, but those with lower risk ratios have a better chance of remaining operational. For instance, while 6 of the 18 closed exchanges have risk ratios below 1, 12 of the 22 open ones do.

4 Regression Analysis of Exchange Breaches

While we cannot conclude that security breaches trigger exchanges to close, we can examine whether any other factors affect the likelihood an exchange will suffer a breach.

4.1 Statistical Model

We use a logistic regression model with a dependent variable denoting whether or not an exchange experiences a breach. We hypothesize that two explanatory variables influence whether a breach occurs:

Average daily transaction volume: bigger exchanges make richer targets. As an exchange processes more transactions, more wealth flows into its accounts. Consequently, we expect that profit-motivated criminals are naturally drawn to exchanges with higher average daily transaction volumes.

Months operational: every day an exchange is operational is another day that it could be hacked. Longer-lived exchanges, therefore, are more exposed to breaches.

The model takes the following form:

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

The dependent variable p_b is the probability that an exchange experiences a security breach, c_0, c_1, c_2 are best-fit constants, $\log(\text{daily vol.})$ is the log-transformed daily transaction volume at the exchange, # months operational is the time (in months) that the exchange has been operational, and ε is an error term.

4.2 Results

The logistic regression yields the following results:

	coef.	Odds-ratio	95% conf. int.	Significance
Intercept	-4.304	0.014	(0.0002,0.211)	$p = 0.0131$
log(Daily vol.)	0.514	1.672	(1.183,2.854)	$p = 0.0176$
Months operational	-0.104	0.901	(0.771,1.025)	$p = 0.1400$
Model fit: $\chi^2 = 10.3, p = 0.00579$				

Transaction volume is positively correlated with experiencing a breach. Months operational, meanwhile, is negatively correlated with being breached, but the association just falls short of statistical significance ($p = 0.14$). Thus, we face a conundrum: according to the results of Section 3, high-volume exchanges are less likely to close but *more likely* to experience a breach. Bitcoin holders can choose to do business with less popular exchanges to reduce the risk of losing money due to a breach, or with more popular exchanges that may be breached, but are less likely to shut down without warning.

Figure 2 takes the coefficients for a best-fit logit model and plots the probability that an exchange operational for the average duration of one year will be breached as transaction volume increases. For example, exchanges handling 275 Bitcoins' worth of transactions each day have a 20% chance of being breached, compared to a 70% chance for exchanges processing daily transactions worth 5570 Bitcoins.

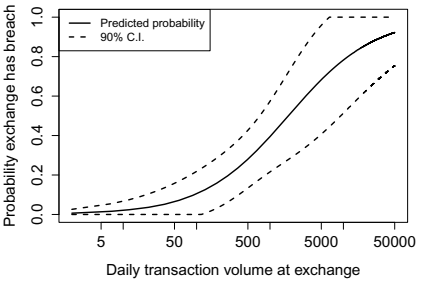

Fig. 2. Probability that an exchange will experience a breach as the average volume of Bitcoins exchanged varies, according to the best-fit logit model.

5 Related Work

Bitcoin's recent success has piqued the interest of a number of researchers in studying it. A couple of works looked into the cryptographic aspects [15, 16, 17] and ways to either improve or build on Bitcoin. Another set of papers explored the Bitcoin network of transactions [18, 19], and documented practical uses of Bitcoin [7]. Others yet investigated economic considerations regarding, in particular, the economic costs of proof-of-work mechanisms such as Bitcoin [20]. Different from these related efforts, we believe our paper is the first to focus on Bitcoin exchanges.

6 Discussion

In this paper, we empirically investigated two risks linked to Bitcoin exchanges. We conducted a survival analysis on 40 Bitcoin exchanges, which found that an exchange's average transaction volume is negatively correlated with the probability it will close prematurely. We also presented a regression analysis which found that, in contrast to the survival analysis, transaction volume is positively correlated with experiencing a breach. Hence, the continued operation of an exchange depends on running a high transaction volume, which makes the exchange a more valuable target to thieves.

Our statistical analysis presents three notable limitations. First, there is substantial randomness affecting when an exchange closes or is breached that is not captured by our model. Future work might investigate additional explanatory variables, such as the exchange reputation. Second, some explanatory variables did not achieve statistical significance due to the data set's modest size. The analysis is worth revisiting as time passes and new exchanges are opened and old ones close. Third, some indicators may need to be changed as Bitcoin grows. For instance, rapid increases in transaction volumes may render long-term unweighted averages less meaningful.

Finally, we focused on economic considerations, such as closure risks, that a rational actor would want to estimate before investing in a given exchange. However, reducing Bitcoin to a mere speculative instrument misses an important piece of the puzzle. Most Bitcoin users are early adopters, often motivated by non-economic considerations. For instance, Silk Road users, who constitute a large share of the Bitcoin economy [7], may shy away from exchanges that require identification, and instead prefer assurances of anonymity. This may in turn lead them to use exchanges posing greater economic risk. Studying the unique characteristics of Bitcoin users and investors, compared to typical foreign exchange traders, is an avenue for future work we think well worth exploring.

Acknowledgments. We thank Rainer Böhme and our anonymous reviewers for their extensive feedback on an earlier version of this paper. This research was partially supported by the National Science Foundation under ITR award CCF-0424422 (TRUST).

References

1. Birch, D., McEvoy, N.: Electronic cash – technology will denationalise money. In: Luby, M., Rolim, J.D.P., Serna, M. (eds.) FC 1997. LNCS, vol. 1318, pp. 95–108. Springer, Heidelberg (1997)
2. Chaum, D.: Achieving electronic privacy. Scientific American, 96–101 (August 1992)
3. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2009), http://www.bitcoin.org/bitcoin.pdf
4. Bitcoin Watch, http://bitcoinwatch.com/ (last accessed January 27, 2013)
5. Leyden, J.: Linode hackers escape with $70k in daring Bitcoin heist. The Register (March 2012), http://www.theregister.co.uk/2012/03/02/linode_bitcoin_heist/
6. Lee, T.: Hacker steals $250k in bitcoins from online exchange bitfloor. Ars Technica (September 2012), http://arstechnica.com/tech-policy/2012/09/hacker-steals-250k-in-bitcoins-from-online-exchange-bitfloor/

7. Christin, N.: Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Technical Report CMU-CyLab-12-018, Carnegie Mellon University (2012)
8. Jeffries, A.: Suspected multi-million dollar Bitcoin pyramid scheme shuts down, investors revolt. The Verge (August 2012), http://www.theverge.com/2012/8/27/3271637/bitcoin-savings-trust-pyramid-scheme-shuts-down
9. Anderson, R.: Closing the phishing hole: Fraud, risk and nonbanks. In: Federal Reserve Bank of Kansas City – Payment System Research Conferences (2007)
10. Moore, T., Han, J., Clayton, R.: The postmodern Ponzi scheme: Empirical analysis of high-yield investment programs. In: Keromytis, A.D. (ed.) FC 2012. LNCS, vol. 7397, pp. 41–56. Springer, Heidelberg (2012)
11. Bitcoin wiki, https://bitcointalk.org/ (last accessed January 27, 2013)
12. Bitcoin forums, https://en.bitcoin.it/ (last accessed January 27, 2013)
13. Yepes, C.: Compliance with the AML/CFT international standard: Lessons from a cross-country analysis. IMF Working Papers 11/177, International Monetary Fund (July 2011)
14. Cox, D.: Regression models and life-tables. Journal of the Royal Statistics Society, Series B 34, 187–220 (1972)
15. Clark, J., Essex, A.: CommitCoin: Carbon dating commitments with bitcoin (short paper). In: Keromytis, A.D. (ed.) FC 2012. LNCS, vol. 7397, pp. 390–398. Springer, Heidelberg (2012)
16. Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better – how to make Bitcoin a better currency. In: Keromytis, A.D. (ed.) FC 2012. LNCS, vol. 7397, pp. 399–414. Springer, Heidelberg (2012)
17. 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)
18. Ron, D., Shamir, A.: Quantitative analysis of the full Bitcoin transaction graph, Cryptology ePrint Archive, Report 2012/584 (October 2012)
19. Reid, F., Harrigan, M.: An analysis of anonymity in the Bitcoin system, arXiv:1107.452a4v2 [physics.soc-ph] (May 2012), http://arxiv.org/abs/1107.4524
20. Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H.P., Böhme, R.: Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In: Proc. WEIS, Berlin, Germany (June 2012)