Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk

Tyler Moore[1] Nicolas Christin[2]

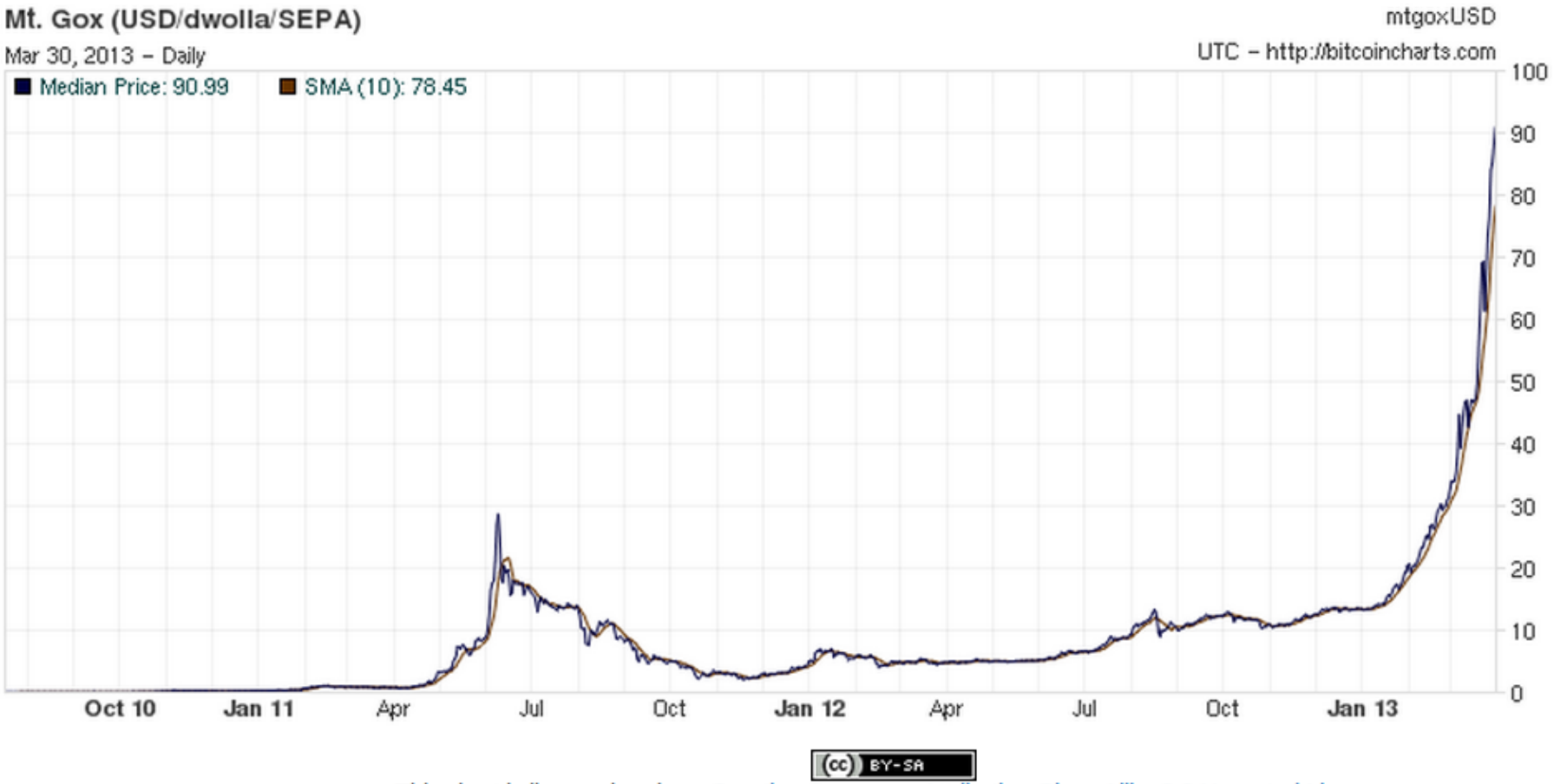
[1] Computer Science & Engineering, Southern Methodist University, USA, tylerm@smu.edu
[2] INI & CyLab, Carnegie Mellon University, USA, nicolasc@cmu.edu

Financial Crypto 2013
Okinawa, Japan
April 2, 2013

SMU. BOBBY B. LYLE SCHOOL OF ENGINEERING

bitcoincharts.com/charts/mtgoxUSD#tgMza1gSMAzm1g10zm2g25

Link to this chart · Larger chart



K.K. Tibanne [JP] https://mtgox.com

Last price:$93.30000 High:$93.80000 Low:$91.00000 Volume:20525 BTC Weighted Avg:$92.72940 USD

MT.GOX

Username Password Login

or Sign up

Trade with confidence on the world's largest Bitcoin exchange!

Mt.Gox is the world's most established Bitcoin exchange. You can quickly and securely trade bitcoins with other people around the world with your local currency!

SIGN UP NOW

"As of July 2011, Mt. Gox handles over 80% of all Bitcoin trade"

WIKIPEDIA

Payments made easy.

Linode hackers escape with $70K in daring bitcoin heist

Compromised servers ransacked for digital cash

By **John Leyden** • **Get more from this author**

Posted in Security, 2nd March 2012 17:05 GMT

Updated Popular web host Linode has been hacked by cyber-thieves who made off with a stash of bitcoins worth $71,000 (£44,736) in real money.

The crooks pulled off the heist after obtaining admin passwords for Linode's network gear. Having infiltrated its systems, the thieves proceeded to target several Bitcoin-related servers, stealing $15k (£9.45k) from one merchant and more than 10,000 bitcoins ($56k, £35k) from Bitcoinica, a trading exchange for the digital currency. Bitcoinica has promised to reimburse customers for any losses. It said in a statement:

> **Many of you have heard that several bitcoin services were victims of a recent Linode security breach today. Unfortunately, Bitcoinica is also among the services affected.**


Hacker steals $250k in Bit
arstechnica.com/tech-policy/2012/09/hacker-steals-250k-in-bitcoins-from-online-exchange-bitfloor/
ars technica
MAIN MENU
MY STORIES: 25
FORUMS
SUBSCRIBE NOW
LAW & DISORDER / CIVILIZATION & DISCONTENTS
Hacker steals $250k in Bitcoins from online exchange Bitfloor
Irreversible transactions make Bitcoin security a high-stakes business.
by Timothy B. Lee - Sept 4 2012, 8:20pm CDT
INTERNET CRIME
88
The future of the up-and-coming Bitcoin exchange Bitfloor was thrown into question Tuesday when the company's founder reported that someone had compromised his servers and made off with about 24,000 Bitcoins, worth almost a quarter-million dollars. The exchange no longer has enough cash to cover all of its deposits, and it has suspended its operations while it considers its options.
Bitfloor is not the first Bitcoin service brought low by hackers. Last year, the most popular Bitcoin exchange, Mt.Gox, suspended operations for a week after an attacker compromised a user account

138

The largest Bitcoin exchange in Brazil gets hacked: depositors are not guaranteed to get their money back (self.Bitcoin)

submitted 1 day ago by avsa

Disclaimer: I'm not associated in any form with Mercado Bitcoin other than having done trades there. Luckily for me I didn't have any money there at the moment.

Mercado Bitcoin, the largest – and only – bitcoin exchange in Brazil, has been offline for almost a week now. For the first few days there was no communication, but the owner just sent an email to all accounts explaining he was hacked. I haven't seen it posted anywhere in English so I'll do my best to translate what I got.

As far as I understood, someone hacked his "redeem code" feature, being able to generate false credits in the system. Then during the night the hacker moved out all his credit into bitcoins, leaving MercadoBitcoin without enough BTC to pay back all the other depositors.

Mercado hasn't revealed how much was robbed or more details than that, but has said he will try to pay back what he can, in that order:

1. Withdraws in Reais that were requested before the attack
2. Deposits in Reais that hadn't been credited yet
3. Current balances in Reais
4. Current balances in Bitcoins

Meaning that depending on how much was left, bitcoin balances will only be given back if he is able to pay back all the money (in Reais) to other creditors, and even that money isn't fully guaranteed.

https://bitcointalk.org/index.php?topic=5441.msg1413156#msg1413156

M4v3R
Hero Member

Posts: 524

Ignore

Re: BitMarket.Eu - ownership changed (in a way)

December 21, 2012, 08:53:16 AM

#518

Hello all. I'm terrible sorry for not responding to this earlier. A mix of personal issues with searching for a solution prevented me from it.

Unfortunately, I have very bad news. I cannot currently proccess your withdrawals. The situation is very complicated and it's all my fault, that's why I feel terrible about it. I tried to make this up, to keep the site afloat and somehow recover the funds, but it's not possible anymore. Right now there are 1786 BTC pending withdrawal, which I can't honor...

Earlier this year, I had this "genius" idea which led me to making a fatal mistake. I thought I could provide a hedge fund service for Bitmarket users. There were other sites providing this service so I guesses that it could be successful. I had experience in trading before, all I needed is a platform. And there was one - Bitcoinica. I was so convinced with this idea (and sooo wrong in hindsight) that for a while I kept majority of "offline" Bitmarket funds there. What I didn't expect was that one day it could just dissapear - taking all the money with it. What's worse, the funds were shorted when it happened (converted to USD and sold) - and after Bitcoinica dissapeared BTC price rose by about 250% until now. So while there is still chance to recover the funds (there is an appointed liquidator assigned to this case and I've already sent in claims) it will be not enough to cover all people's funds. For the record - there are ~~20161~~ 18787.72139217 BTC missing (edit: I subtracted my funds that also were deposited on Bitmarket), and Bitcoinica claims total for around 50K USD (the exact amount is uncertain because the liquidators haven't yet stated at what rate they will liquidate positions).

Sadly, I alone, I'm out of options. I don't have own money to pay for this loss (Bitmarket never made any real profit and I make up for a living by part-time web/mobile programming). The options for making this up for everyone as I see are:

- find an investor (or investors) that is willing to cover at least part of is debt. I would transfer all rights to the website software, servers and database to him and also work as a technician, possibly also implementing features he'd wanted. If you reading this have the funds necessary to make this work, PLEASE contact me on this.
- freeze all current funds and "start over" trading with explicit fees, implementing much-needed features like rating system and others. All profits from the fees would go directly to a fund for repaying the debt. I'm afraid that this option

https://bitcointalk.org/index.php?topic=94649.0

cryptoanarchist
Hero Member

Posts: 554

Ignore

Re: btcex "Maintenance"?
July 25, 2012, 03:56:14 PM #9

> **Quote from: ewibit on July 25, 2012, 10:37:07 AM**
>
> > **Quote from: starsoccer9 on July 24, 2012, 07:50:32 PM**
> >
> > it was having horrible problems with not being able to withdraw btc.
> > I personally think the site is closed and wont be reopening. I hope it does i liked the exchange.
>
> last time Jul 21, 2012 I have had the same problem - I was not able to withdraw my BTC's ...
> I hope the site does reopening
> or
> how can I get back my BTC's and money soon?
> TIA

Think were just screwed.

starsoccer9
Full Member

Posts: 224

Ignore

Re: btcex "Maintenance"?
July 25, 2012, 08:45:45 PM #10

Same, A couple people told me that the owner was a scammer so it would kinda make sense. I really hope not but it would make alot of sense if he did. He was waiting for 10000 btc and finnaly hit it and locked everyones btc in aswell

Motivation

- Decentralization is a key feature of Bitcoin's design
- Viewed as a security benefit: protects against inflation risk, sovereign risk, etc.
- Yet an extensive ecosystem of **3rd-party intermediaries** now supports Bitcoin transactions: currency exchanges, escrow services, online wallets, mining pools, investment services, ...
- Most risk Bitcoin holders face stems from interacting with these intermediaries, who act as **de facto central authorities**
- We focus on risk posed by **failures of currency exchanges**

Motivation

- Decentralization is a key feature of Bitcoin's design
- Viewed as a security benefit: protects against inflation risk, sovereign risk, etc.
- Yet an extensive ecosystem of **3rd-party intermediaries** now supports Bitcoin transactions: currency exchanges, escrow services, online wallets, mining pools, investment services, ...
- Most risk Bitcoin holders face stems from interacting with these intermediaries, who act as **de facto central authorities**
- We focus on risk posed by **failures of currency exchanges**

Motivation

- Decentralization is a key feature of Bitcoin's design
- Viewed as a security benefit: protects against inflation risk, sovereign risk, etc.
- Yet an extensive ecosystem of **3rd-party intermediaries** now supports Bitcoin transactions: currency exchanges, escrow services, online wallets, mining pools, investment services, ...
- Most risk Bitcoin holders face stems from interacting with these intermediaries, who act as **de facto central authorities**
- We focus on risk posed by **failures of currency exchanges**

Outline of today's talk

1. Data on Bitcoin-Exchange Closures
   - Data Collection Methodology
   - Summary Statistics
2. Survival Analysis of Exchange Closure
   - Statistical Model
   - Results
   - Risk Ratio for Bitcoin Exchanges
3. Regression Analysis of Exchange Breaches
   - Statistical Model
   - Results

Outline

Data collection methodology

- Data sources
  1. Daily transaction volume data on 40 exchanges converting into 33 currencies from `bitcoincharts.com`
  2. Checked for closure, mention of security breaches and whether investors were repaid on Bitcoin Wiki and forums
  3. To assess impact of pressure from financial regulators, we identified each exchange's country of incorporation and used a World Bank index on compliance with anti-money laundering regulations
- Key measure: exchange lifetime
  - Time difference between first and last observed trade
  - We deem an exchange closed if no transactions are observed at least 2 weeks before data collection finished

Some initial summary statistics

- 40 Bitcoin currency exchanges opened since 2010
- 18 have subsequently closed (45% failure rate)
  - Median lifetime is 381 days
  - 45% of closed exchanges did not reimburse customers
- 9 exchanges were breached (5 closed)

18 closed Bitcoin currency exchanges

Exchange	Origin	Dates Active	Daily vol.	Closed?	Breached?	Repaid?	AML
BitcoinMarket	US	4/10 – 6/11	2454	yes	yes	–	34.3
Bitomat	PL	4/11 – 8/11	758	yes	yes	yes	21.7
FreshBTC	PL	8/11 – 9/11	3	yes	no	–	21.7
Bitcoin7	US/BG	6/11 – 10/11	528	yes	yes	no	33.3
ExchangeBitCoins.com	US	6/11 – 10/11	551	yes	no	–	34.3
Bitchange.pl	PL	8/11 – 10/11	380	yes	no	–	21.7
Brasil Bitcoin Market	BR	9/11 – 11/11	0	yes	no	–	24.3
Aqoin	ES	9/11 – 11/11	11	yes	no	–	30.7
Global Bitcoin Exchange	?	9/11 – 1/12	14	yes	no	–	27.9
Bitcoin2Cash	US	4/11 - 1/12	18	yes	no	–	34.3
TradeHill	US	6/11 - 2/12	5082	yes	yes	yes	34.3
World Bitcoin Exchange	AU	8/11 – 2/12	220	yes	yes	no	25.7
Ruxum	US	6/11 – 4/12	37	yes	no	yes	34.3
btctree	US/CN	5/12 – 7/12	75	yes	no	yes	29.2
btcex.com	RU	9/10 – 7/12	528	yes	no	no	27.7
IMCEX.com	SC	7/11 – 10/12	2	yes	no	–	11.9
Crypto X Change	AU	11/11 – 11/12	874	yes	no	–	25.7
Bitmarket.eu	PL	4/11 – 12/12	33	yes	no	no	21.7

22 open Bitcoin currency exchanges

Exchange	Origin	Dates Active	Daily vol.	Closed?	Breached?	Repaid?	AML
bitNZ	NZ	9/11 – pres.	27	no	no	–	21.3
ICBIT Stock Exchange	SE	3/12 – pres.	3	no	no	–	27.0
WeExchange	US/AU	10/11 – pres.	2	no	no	–	30.0
Vircurex	US?	12/11 – pres.	6	no	yes	–	27.9
btc-e.com	BG	8/11 – pres.	2604	no	yes	yes	32.3
Mercado Bitcoin	BR	7/11 – pres.	67	no	no	–	24.3
Canadian Virtual Exchange	CA	6/11 – pres.	832	no	no	–	25.0
btcchina.com	CN	6/11 – pres.	473	no	no	–	24.0
bitcoin-24.com	DE	5/12 – pres.	924	no	no	–	26.0
VirWox	DE	4/11 – pres.	1668	no	no	–	26.0
Bitcoin.de	DE	8/11 – pres.	1204	no	no	–	26.0
Bitcoin Central	FR	1/11 – pres.	118	no	no	–	31.7
Mt. Gox	JP	7/10 – pres.	43230	no	yes	yes	22.7
Bitcurex	PL	7/12 – pres.	157	no	no	–	21.7
Kapiton	SE	4/12 – pres.	160	no	no	–	27.0
bitstamp	SL	9/11 – pres.	1274	no	no	–	35.3
InterSango	UK	7/11 – pres.	2741	no	no	–	35.3
Bitfloor	US	5/12 – pres.	816	no	yes	no	34.3
Camp BX	US	7/11 – pres.	622	no	no	–	34.3
The Rock Trading Company	US	6/11 – pres.	52	no	no	–	34.3
bitme	US	7/12 – pres.	77	no	no	–	34.3
FYB-SG	SG	1/13 – pres.	3	no	no	–	33.7

Outline

What factors affect whether an exchange closes?

- We hypothesize three variables affect survival time for a Bitcoin exchange
  1. **Average daily transaction volume** (positive)
  2. **Experiencing security breach** (negative)
  3. **AML/CFT compliance** (negative)
- Since lifetimes are censored, we construct a Cox proportional hazards model:

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

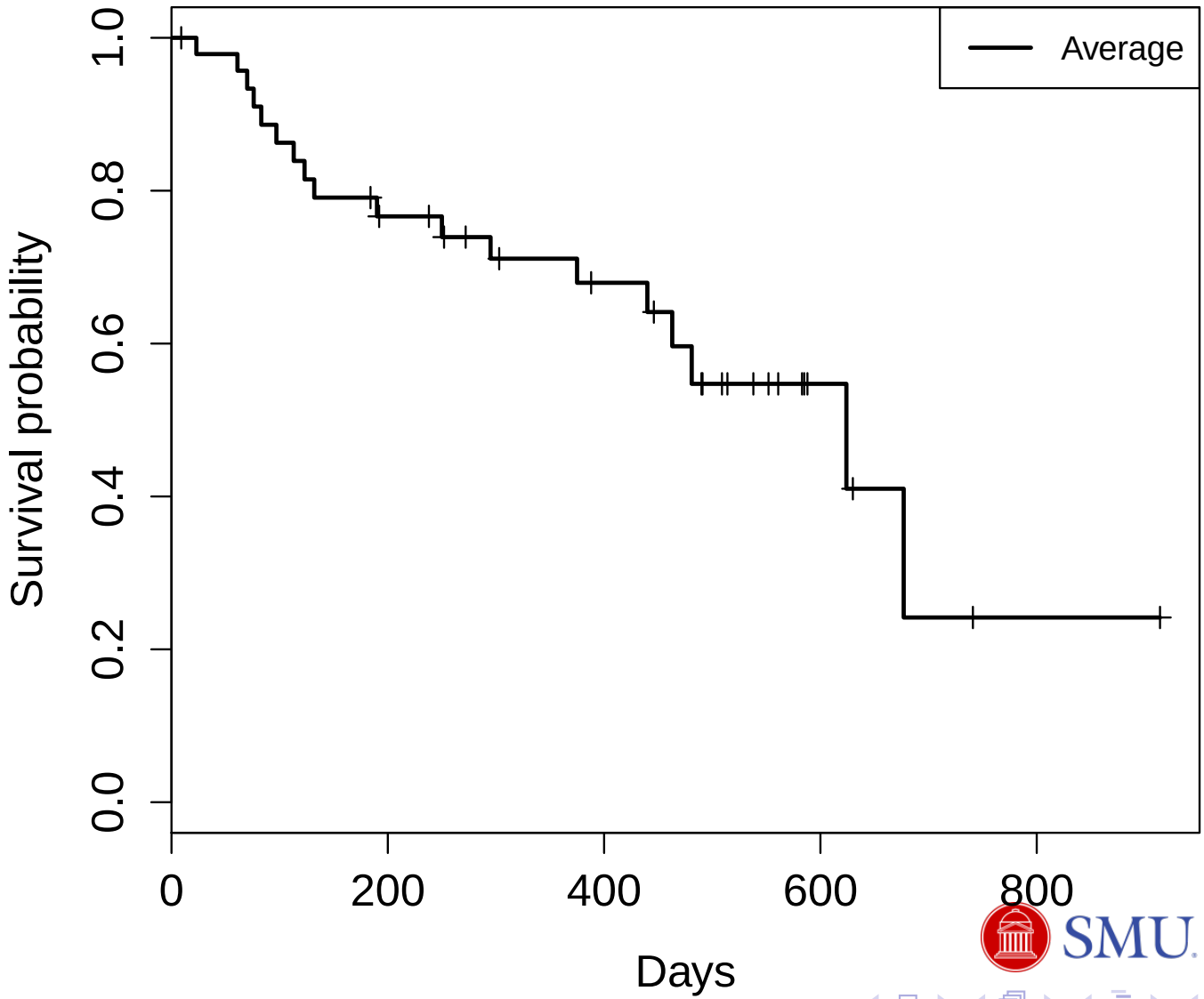
Cox proportional hazards model: results

		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	$p = 0.9221$

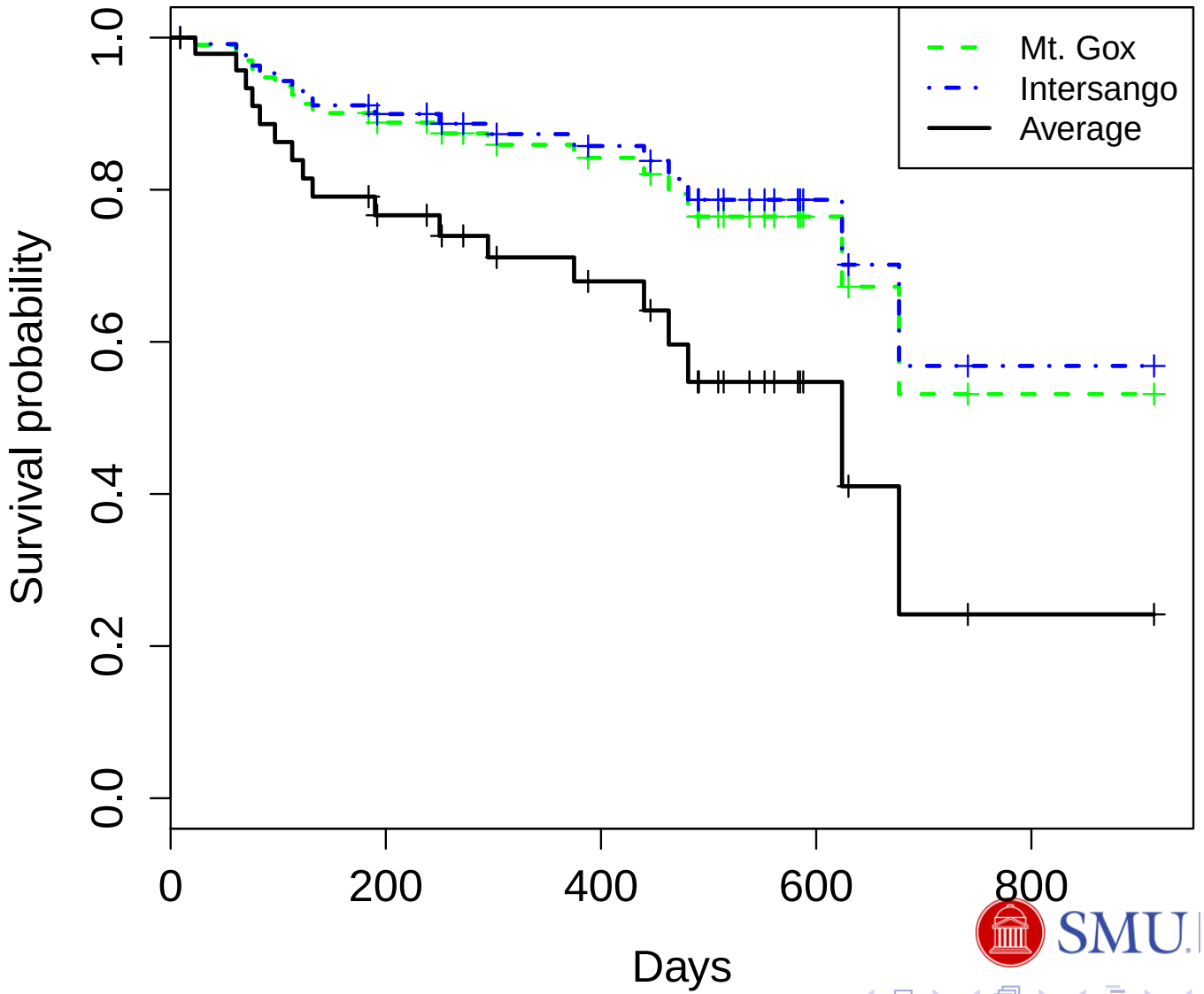
log-rank test: Q=7.01 ($p = 0.0715$), $R^2 = 0.145$

- Higher daily transaction volumes associated with longer survival times (statistically significant)
- Experiencing a breach associated with shorter survival times (not quite statistically significant)

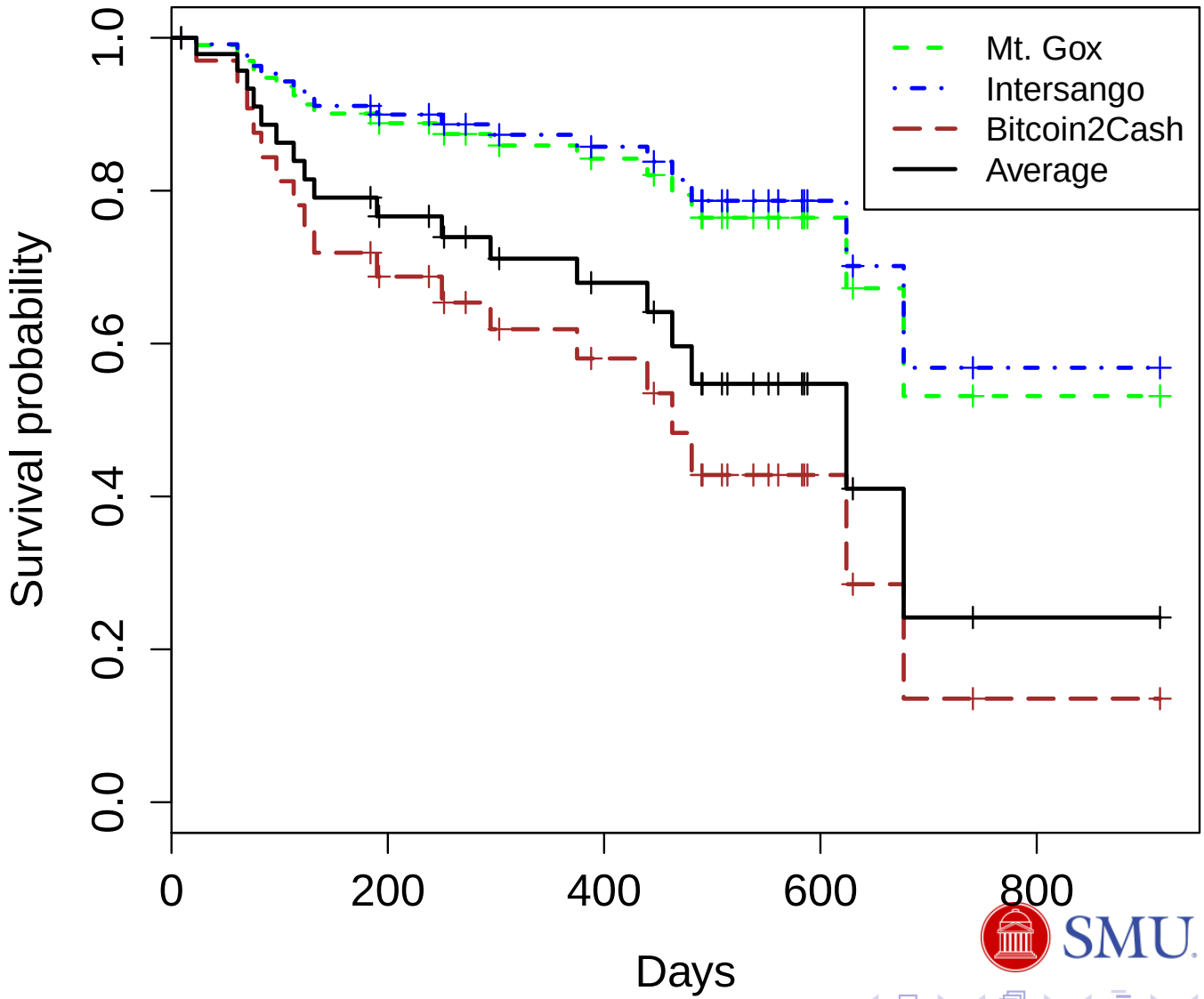
Survival probability for Bitcoin exchanges



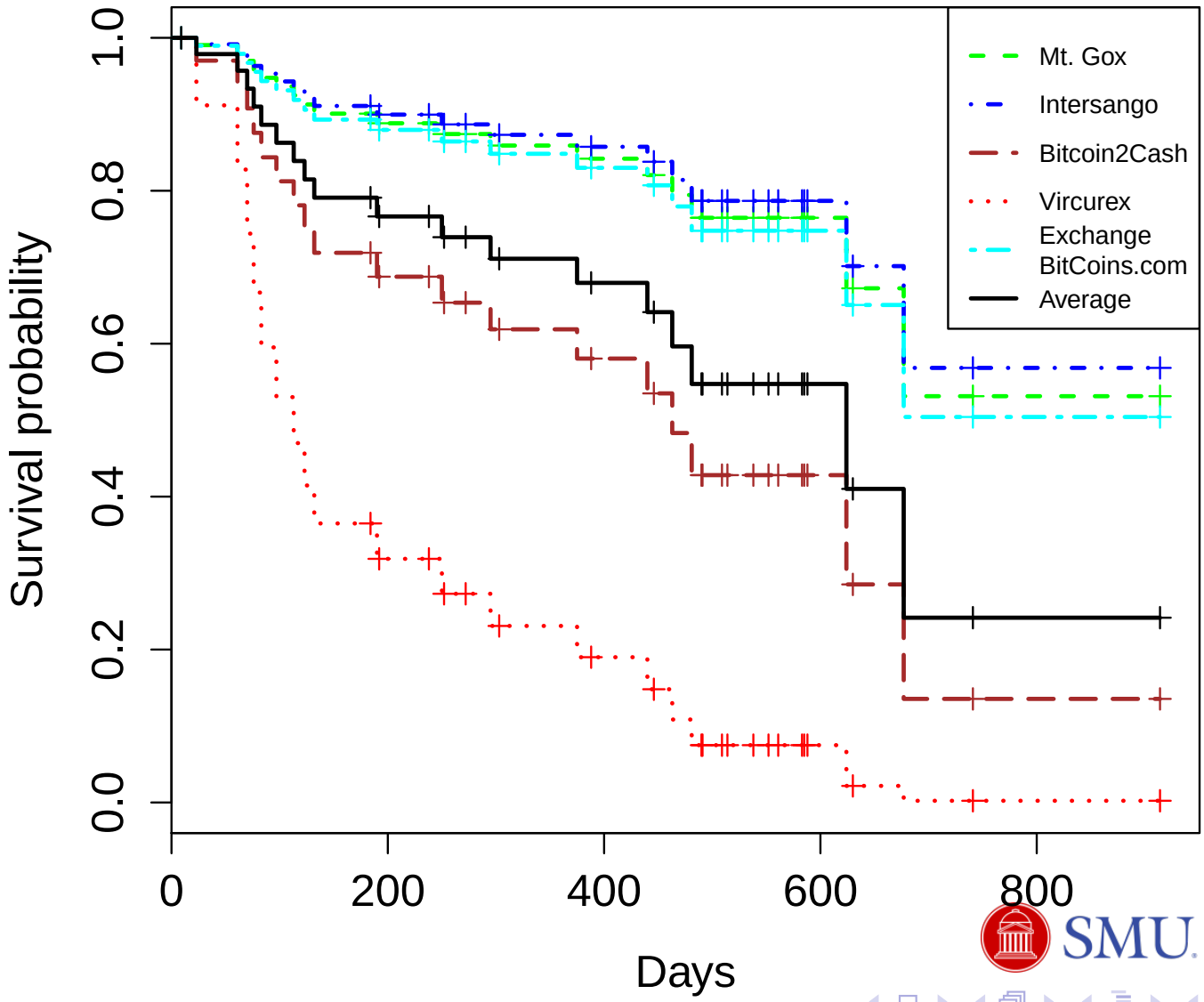
High-volume exchanges have better chance to survive



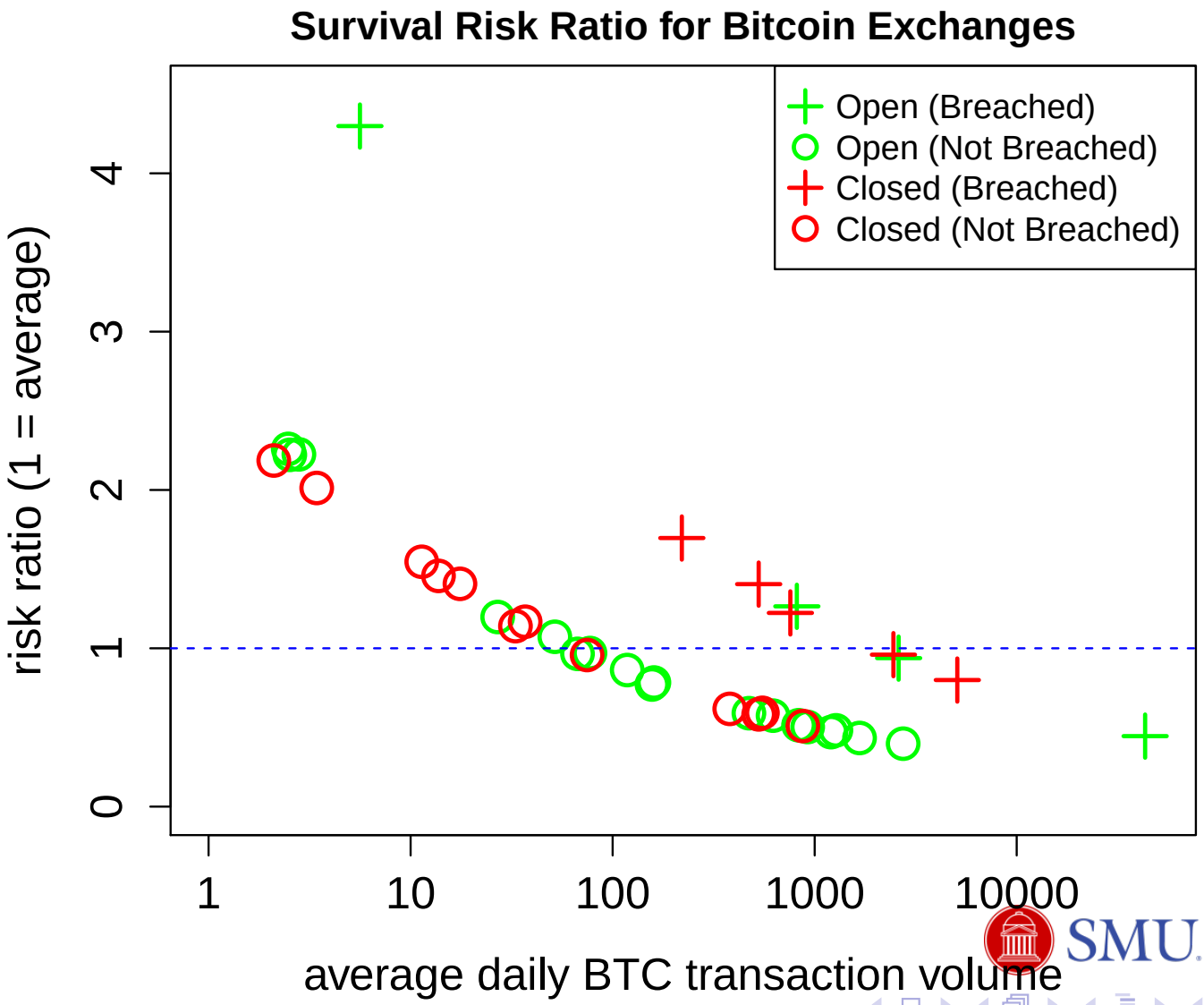
Low-volume exchanges have worse chance to survive



Yet some lower-risk exchanges collapse, high-risk survive



Risk ratio for all 40 exchanges



Outline

What factors affect whether an exchange is breached?

- We hypothesize three variables affect whether a Bitcoin exchange loses money from a security breach
  1. **Average daily transaction volume** (positive)
  2. **Months operational** (positive)
- We use a logistic regression model with a dependent variable denoting whether or not an exchange experiences a breach:

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

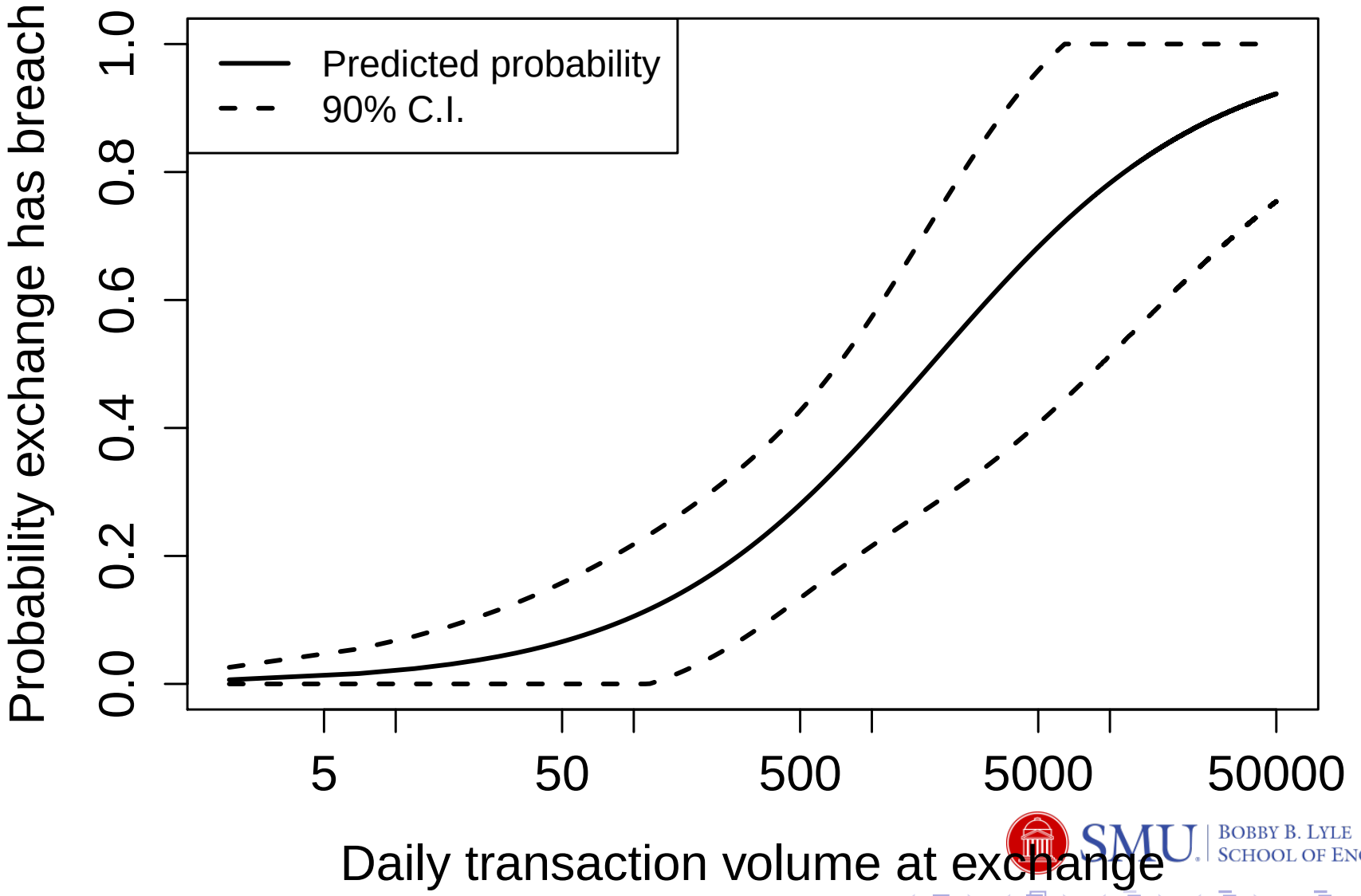
Logistic regression for exchange breaches

	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 (statistically significant)
- Months operational is negatively correlated with being breached (not quite statistically significant)

SMU | Bobby B. Lyle School of Engineering

Breach probability as a function of daily transaction volume



Concluding remarks (1)

- Currency exchanges pose substantial risk to Bitcoin holders: 45% of exchanges have closed, often leaving customers unable to withdraw stored funds
- Using survival analysis, we found that an exchange's average transaction volume is negatively correlated with the probability it will close prematurely
- Using regression, we found that 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

Concluding remarks (2)

- Limitations to the statistical analysis
  1. There is substantial randomness affecting when an exchange closes or is breached that is not captured by our mode
  2. Some of the explanatory variables did not achieve statistical significance due to the dataset's modest size
- We focus on economic considerations, such as closure risk, that a rational actor should consider before transacting with an exchange
- But behavioral factors may explain participation better (e.g., Silk Road customers want exchanges that respect anonymity)
- Paper: `http://lyle.smu.edu/~tylerm/fc13.pdf`