



Online-Appendix zu

„The Influence of Cryptocurrencies on Enterprise Risk Management – an empirical evidence by the example of Bitcoin“

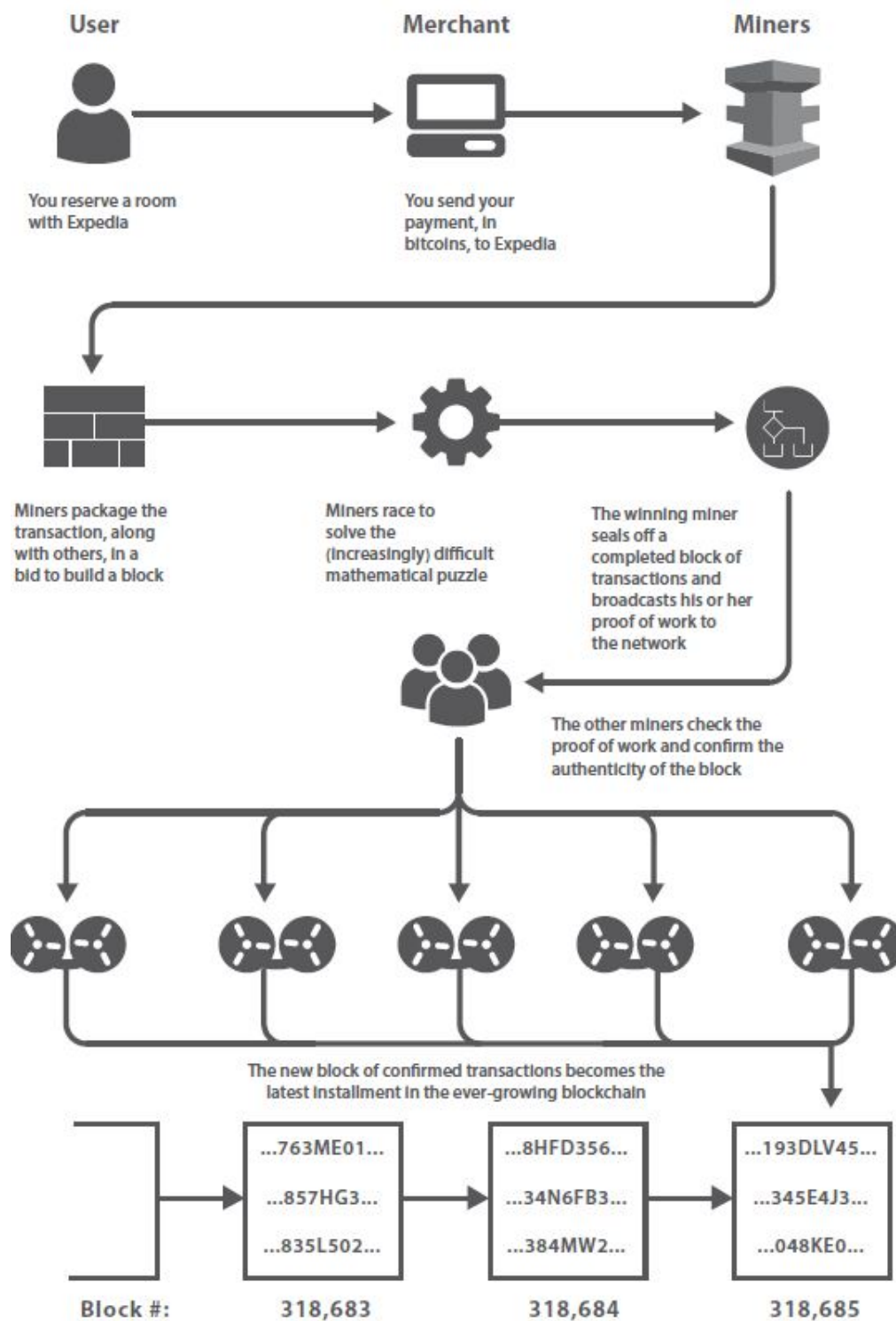
Maximilian Böstler

Universität St. Gallen

Junior Management Science 4(2) (2019) 195-227

Appendices

Appendix 1: Overview of the Bitcoin Mining Process



Source: Own illustration according to Vigna & Casey, 2016, p. 126

Appendix 2: Price Development of Bitcoin/USD



Source: Bloomberg, 2018

Appendix 3: COSO IC Framework Principles

Component	Principle	Fundamental Concepts
Control Environmet	1	The organization demonstrates a commitment to integrity and ethical values.
	2	The board of directors demonstrates independence from management and excercises oversight of the development and performance of internal control.
	3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilites in the pursuit of objectives.
	4	The organization demonstrates a commitment to attract, develop, and retain compatent individuals in alignment with objectives.
	5	The organization hold individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	6	The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	7	The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determing how the risks should be managed.
	8	The organization considers the potential for fraud in assessing risks to the achievement of objectives.
	9	The organization identifies and assesses changes that could significantly impact the system of internal control.
Control Activities	10	The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	11	The organization selects and develops general control activities over technology to support the achievement of objectives.
	12	The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
Information & Communication	13	The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
	14	The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	15	The organization communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring Activities	16	The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	17	The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior managment and the board of directors, as appropriate.

Source: Own illustration according to COSO, 2013, pp. 6-7

Appendix 4: Correspondence

Bachelorarbeitsstudie zum Thema Riskomanagement von Kryptowährungen / Bachelor's thesis survey concerning the risk management of cryptocurrencies



Boelstler, Maximilian
Mi 22.11.2017, 12:20



Allen antworten | v

Gesendete Elemente

English version below

Sehr geehrte Damen und Herren [REDACTED]

Im Rahmen meiner Bachelorarbeit am Lehrstuhl für Internal Audit/ Internal Control – Institut für Accounting, Controlling und Auditing (ACA) – an der Universität St. Gallen (Referent Prof. T. Flemming Ruud, PhD) untersuche ich die *Risiken von Kryptowährungen am Beispiel des Bitcoins* sowie deren Handhabung in den operationalen Geschäftspraktiken, wie z.B. der Zahlungsabwicklung.

Da Ihr Unternehmen auf der Plattform www.btc-echo.de als Bitcoin Akzeptanzstelle gelistet ist, stellen Sie eine repräsentative Organisation für diese Untersuchung dar. In diesem Sinne wäre ich Ihnen sehr dankbar, wenn Sie sich **8-12 Minuten** Zeit nehmen und die folgende Umfrage hinsichtlich Ihres Umgangs mit Bitcoinzahlungen **bis zum 15.12.2017** beantworten:

<http://uu293a.findmind.ch/?l=0>

Die Umfrage wird selbstverständlich vertraulich ausgewertet. Im Gegenzug für Ihr entgegengebrachtes Engagement, kann ich Ihnen meine Ergebnisse bis Anfang Juni 2018 zur Verfügung stellen. Ich hoffe, dass ich Ihnen sowie Ihrem Unternehmen spannende Einblicke sowie praktikable Empfehlungen im Umgang mit Kryptowährungen ermöglichen kann.

Für Rückfragen stehe ich Ihnen jederzeit unter der folgenden Mailadresse zur Verfügung:
maximilian.boelstler@student.unisg.ch

Ein herzliches Dankeschön vorab und freundliche Grüsse
Maximilian Bölstler

Dear Sir or Madam [REDACTED]

Within the scope of my current bachelor thesis at the chair of internal audit/ internal control – institute for accounting, controlling and auditing (ACA) – at the University of St. Gallen (supervisor: Prof. T. Flemming Ruud, PhD), I am analyzing the *risks of cryptocurrencies concerning their operational dealing by the example of Bitcoin*, for instance within the payment process.

Due to the fact that your company is registered at www.btc-echo.de as a Bitcoin acceptance venue, your company would be a representative organisation for this analysis. I would be very grateful if you **take 10-12 minutes** to answer the following survey **until the 15th December 2017**:

<http://uu293a.findmind.ch/?l=2>

This survey will be evaluated in a confidential and anonymous manner. In order to say thank you for participating, I might make my results available to you until the beginning of June 2018. In this context, I hope to give you worthwhile insights and feasible recommendations to further improve your operational dealing with cryptocurrencies.

If you have any questions, please do not hesitate to contact me by the following mail:
maximilian.boelstler@student.unisg.ch

Thank you very much in advance for your cooperation.

Kind regards,
Maximilian Bölstler

Appendix 5: Survey

The influence of cryptocurrencies on risk management - an empirical evidence by the example of Bitcoin

Language: English 

Dear Sir or Madam,


Within the scope of my current bachelor at the University of St. Gallen (HSG), I am analysing the risks of cryptocurrencies as a payment method by the example of Bitcoin. This survey aims at investigating the operational dealing of bitcoins (and risks involved) by companies accepting Bitcoin payments. Furthermore, the current coverage of these risks will be examined.

The ultimate goal of this research will be the development of a framework to ensure an appropriate handling of cryptocurrencies as a payment method.

I would be very grateful if you take 8-12 minutes to answer the following questions.

Thank you very much in advance for your cooperation.

Kind regards,
Maximilian Böstler

 [Take Survey](#)

1 – General Questions

In which industry does your organisation operate?

- ☐ banking, insurance, financial sector
- ☐ architecture, real estate, building industry
- ☐ chemical/ biological/ pharmaceutical/ physical industry
- ☐ tourism, catering
- ☐ medical field, healthcare
- ☐ retail, distribution, sale
- ☐ IT
- ☐ logistics
- ☐ management, advisory
- ☐ marketing, PR
- ☐ mechanical engineering, automobile industry, metal construction
- ☐ legal, tax, finance, controlling
- ☐ other services
- ☐ public administration
- ☐ other industry:

Which company size does your organisation assign?

- ☐ micro-businesses (up to 9 employees and up to € 2 million revenue/year)
- ☐ small businesses (up to 49 employees and up to € 10 million revenue/year)
- ☐ small and medium-sized enterprises (up to 249 employees and up to € 50 million revenue/year)
- ☐ large corporations (more than 249 employees and over € 50 million revenue/year)

Why does you, respectively your company, accept Bitcoin payments as an alternative payment method?

multiple responses possible

- ☐ lower transactions cost in comparison to credit card payments
- ☐ Bitcoin is a secure payment option
- ☐ our customers demanded for Bitcoin as a payment method
- ☐ media attraction because of using the slogan "Bitcoin Accepted Here"
- ☐ supporting the concept of Bitcoin
- ☐ attracting Bitcoin supporters as potential clients
- ☐ own response:

How many percent of the total transactions are currently paid with Bitcoin?

In this context, a simple estimation is completely sufficient.

	< 1%	1 - 5%	5 - 20%	20 - 50%	> 50%
percent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2 – Payment Process

Do you use a third-party provider to process your payments? *

Is there any payment processor involved relating the transaction process? In this context it may be mentioned that some of the most common ones are BitPay, Coinify, Coinkite or coinpayments.net. Basically, a payment processor is responsible for the simplification of (Bitcoin) payments. In order to achieve this, a payment processor offers many services around the transaction eg. plugins for the online shop, point-of-sales interfaces or the applications necessary to accept the payments - in return of a percentage fee. Furthermore, some risks can be eliminated respectively minimised by using a payment processor.

☐ yes

☐ no

Do you think the following criteria might represent a risk for the Bitcoin acceptance and the payment processing?

	yes	no
duration of the payment verification (payment confirmation might be not successful)	<input type="radio"/>	<input type="radio"/>
payment documentation & invoicing	<input type="radio"/>	<input type="radio"/>
reporting & tax issues	<input type="radio"/>	<input type="radio"/>
exchange rate risk	<input type="radio"/>	<input type="radio"/>

This question will be only exhibited if the previous question “Do you use a third-party provider to process your payments?” was answered with “no”.

Why do you use a payment processor?

multiple responses possible

- ☐ immediate (automatic) exchange in fiat currencies respectively national currencies
- ☐ providing the infrastructure for Bitcoin payments (shopping cart plugin in the area of eCommerce, Apps & Interface for the point-of-sales)
- ☐ automatic generation of an invoice respectively a sales document
- ☐ enabling the bitcoin acceptance without an in-depth knowledge
- ☐ Bitcoin payments will be confirmed immediately (payment processor is liable for a payment default, ie. if the payment can not be verified)
- ☐ own response:

This question will be only exhibited if the penultimate question “Do you use a third-party provider to process your payments?” was answered with “yes.”

How do you deal with received Bitcoin payments?

multiple responses possible

- ☐ Bitcoins will be changed immediately/ by the following day in national currencies (ie. Bitcoins mainly function as an alternative payment method regarding the payment processing)
 - ☐ Bitcoins will be stored (as an investment)
 - ☐ Bitcoins will be used as liquid funds (eg. to finance further business activities such as the payment of supplier invoices)
 - ☐ own response:
-

3 – Administration & Storage

How are the Bitcoins stored at your company?

- ☐ hot storage
- ☐ cold storage
- ☐ both
- ☐ the Bitcoins are stored in the wallet of my payment processor.
- ☐ I do not know neither hot storage nor cold storage mean. Generally, I have no idea how my Bitcoins are stored.

This question will be only exhibited if the previous question “How do you deal with received Bitcoin payments?” was answered with at least one of the following two options “as an or investment” or “as liquid funds.”

Who has the admission or the relevant access rights to access your company wallet?

position of your employee(s)/ division

amount of employees

comment

In which field of competence could the administration of Bitcoin payments be assigned?

(eg. Chief Executive Officer, Head of Finance, Chief Risk Officer, Intern, ...)

position of the responsible person

4 – Risk Awareness & Evaluation

Evaluate the following criteria concerning their risk potentials in connection with Bitcoin payments

If there are any further risks you were able to observe please complement them in the comment box below.

	no risk	low risk	moderate risk	high risk	extremely high risk	I am not able to evaluate this
a lack of know-how in dealing with cryptocurrencies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
a lack of clear responsibilities in relation with the Bitcoin administration (access, storage, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
price volatility & exchange rate risk of Bitcoins	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
irreversibility of transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
financial reporting risks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
tax risks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
compliance risks (anti-money laundering & know-your-customer issues)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
cyber risks (individual hacking attacks)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
blockchain risks (Bitcoin network will be hacked, implementation of new protocols, double-spending becomes possible, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Evaluate the following criteria concerning their damage potentials on your company in connection with Bitcoin payments

1 - low/ almost no damage potential; 10 - extremely high damage potential

	damage potential/ severity (1 - 10)
a lack of know-how in dealing with cryptocurrencies	<input type="text" value="-"/>
a lack of clear responsibilities in relation with the Bitcoin administration (access, storage, ...)	<input type="text" value="-"/>
price volatility & exchange rate risk of Bitcoins	<input type="text" value="-"/>
irreversibility of transactions	<input type="text" value="-"/>
financial reporting risks	<input type="text" value="-"/>
tax risks	<input type="text" value="-"/>
compliance risks (anti-money laundering & know-your-customer issues)	<input type="text" value="-"/>
cyber risks (individual hacking attacks)	<input type="text" value="-"/>
blockchain risks (Bitcoin network will be hacked, implementation of new protocols, double-spending becomes possible, etc.)	<input type="text" value="-"/>

5 – Control Activities

For the following risks areas the development of internal controls is possible:

An internal control framework “will enable organizations to effectively and efficiently develop and maintain systems of internal control that can enhance the likelihood of achieving the entity’s objectives and adapt to changes in the business and operating environments” (COSO, 2013). Internal controls are any measures (checks, guidelines, controls, ...) to support this process. Based on this definition, only the potential risks and the thus resulting internal controls will be investigated which can be effectively influenced by a company, for instance, the volatility of Bitcoin can not be influenced by the company but the exchange rate risk.

	absolutely possible	rather possible	partially possible	rather not possible	impossible	cannot say
a lack of know-how in dealing with cryptocurrencies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
a lack of clear responsibilities in relation with the Bitcoin administration (access, storage, ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
exchange rate risk of Bitcoins	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
financial reporting risks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
tax issues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
compliance risks (anti-money laundering & know-your-customer issues)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
cyber risks (individual hacking attacks)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Are there currently any internal controls implemented or similar measures in order to ensure an appropriate dealing with Bitcoin payments at your company? *

- ☐ yes
- ☐ no

For the following risks areas the internal controls described below are currently used:

If there are any further controls using in dealing with Bitcoin payments please describe them in the comment box below.

	internal controls
a lack of know-how in dealing with cryptocurrencies	<input type="text"/>
a lack of clear responsibilities in relation with the Bitcoin administration (access, storage, ...)	<input type="text"/>
exchange rate risk of Bitcoins	<input type="text"/>
financial reporting risks	<input type="text"/>
tax issues	<input type="text"/>
compliance risks (anti-money laundering & know-your-customer issues)	<input type="text"/>
cyber risks (individual hacking attacks)	<input type="text"/>

This question will be only exhibited if the previous question “Are there currently any internal controls implemented or similar measures in order to ensure an appropriate dealing with Bitcoin payments at your company?” was answered with “yes.”

6 – Request of Results

Do you like to receive the results of this analysis?

☐ Yes

☐ No

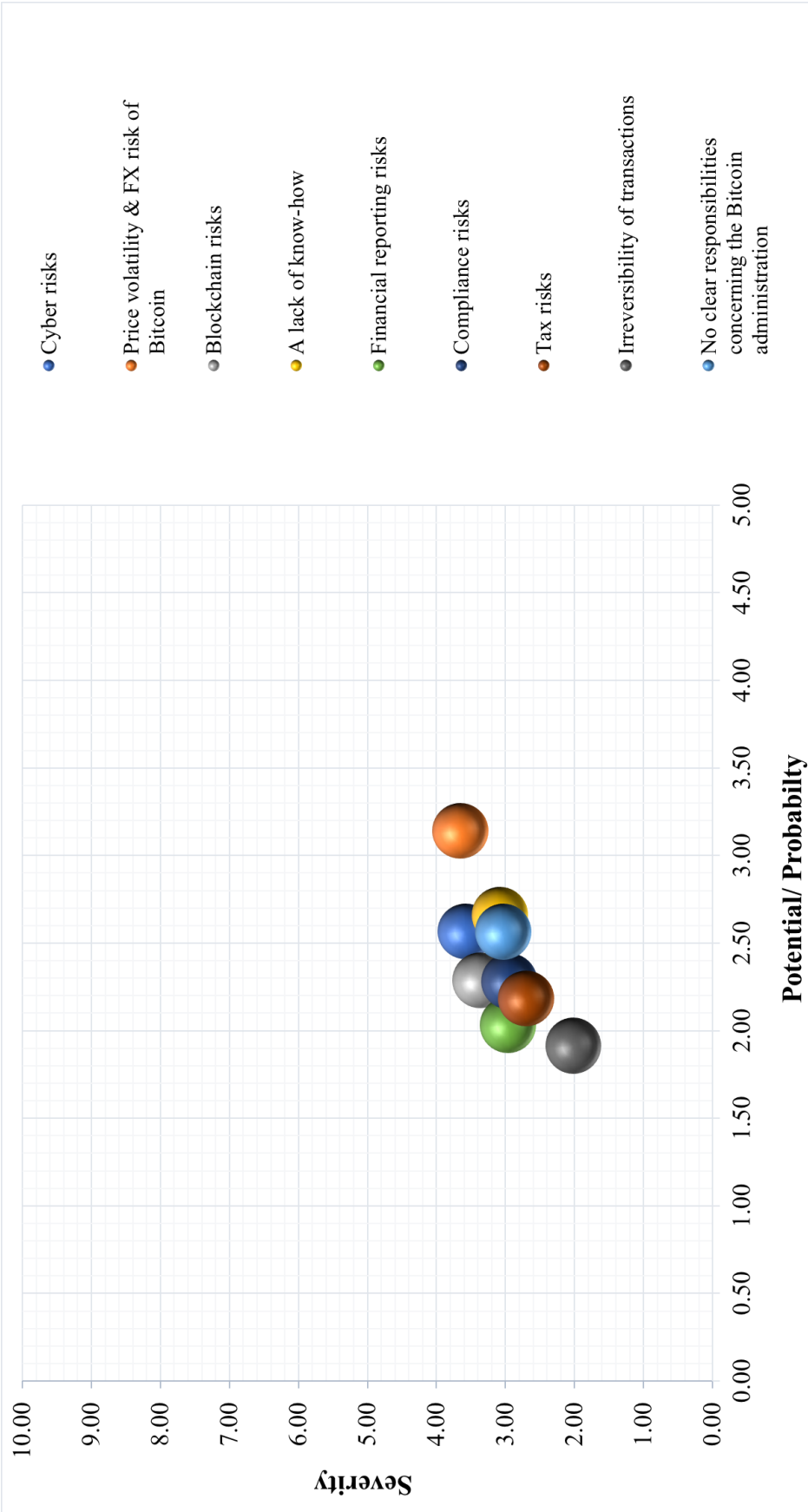
Please type in your email address:

This email address will be used solely for the purpose of sending the survey results.

Mail

This question will be only exhibited if the previous question “Do you like to receive the results of this analysis?” was answered with “yes.”

Appendix 6: Risk Matrix of the Empirical Analysis



Appendix 7: Overview of Implemented Internal Controls

Risk	Internal Controls/ Measures
A lack of know-how in dealing with cryptocurrencies	<ul style="list-style-type: none"> - regular trainings/ workshops - YouTube tutorials - the reading of an established manual is obligated - manuals and internal guidelines
A lack of clear responsibilities in relation with the Bitcoin administration	<ul style="list-style-type: none"> - limiting of responsibilities to a determined, small group of persons, e.g., only the CEO + representative have access - access rights have to be clearly documented - cold storage and/ or an additional pin encryption, for instance by using the software “KeePass”
FX risk of Bitcoin	<ul style="list-style-type: none"> - instant conversion in fiat currencies - documentation of transaction incl. real time exchange rate - observation & documentation of exchange rate
Financial reporting risks	<ul style="list-style-type: none"> - hiring a professional (external) advisor - appropriate documentation - four-eyes principle - no financial reporting because of instant exchange - manual control
Tax risks	<ul style="list-style-type: none"> - appropriate documentation - hiring a professional (external) advisor - manual control - four-eyes principle
Compliance risks	<ul style="list-style-type: none"> - additional KYC check/ identification of customer as part of the ordering process - reporting of suspicious customers - internal assignment of public addresses to (real) customers - own IT-Forensic division - monitoring of applicable national regulation and if necessary, implementing of the relevant actions
Cyber risks	<ul style="list-style-type: none"> - internal IT risk management - internal IT-Forensic division - cold wallets or outsourcing of the private key storage - trainings - software “KeePass”

Appendix 8: Cryptocurrency IC Framework (fine resolution)

