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

Junior Management Science

journal homepage: www.jums.academy

The Influence of Cryptocurrencies on Enterprise Risk Management – An Empirical Evidence by the Example of Bitcoin

Maximilian Bölstler

Universität St. Gallen

Abstract

This thesis analyzes the influence of cryptocurrencies in the context of risk management by considering the emerging risk factors of Bitcoin as a payment method. By means of an empirical analysis through an online survey, the current operational dealing of incoming Bitcoin funds, the risk awareness of the potential threats, and the corresponding control activities implemented by companies accepting Bitcoin payments have been examined. The results reveal that the risks of this new technology-based payment method have not been extensively evaluated and that there exists a partially significant lack of know-how. Therefore, the risks are either not at all or improperly addressed by a majority of the organizations. However, the exchange rate risk and the cyber risk, which is a strongly linked to the administration of cryptocurrencies, represent the most significant related risk factors associated with cryptocurrencies in recent times. To ensure an appropriate operational dealing with cryptocurrencies, the author presents a risk control matrix based on the results of the analysis and discusses control activities to mitigate these emerging threats. Finally, a holistic Cryptocurrency IC Framework (following the COSO 2013 IC Framework) is presented, with the objective of effectively and efficiently developing and maintaining systems of internal control with regard to cryptocurrencies.

Keywords: Blockchain; digital assets; Bitcoin; cryptocurrency; IC framework; enterprise risk management.

1. Introduction

1.1. Problem Statement & Research Questions

The 21st century is characterized by continuous changes and the need for ongoing adaptation, with key terms like "digitization" and "automatization" playing an increasingly important role, particularly in the fast paced environment of a company. These changes can in fact be observed in almost all industries, ranging from manufacturing businesses to service providers. In these modified circumstances, with the emergence of new opportunities, unfamiliar risks and threats have also arisen. It is thus inevitable for companies and their executive management teams to thoroughly think through their implemented business models and, moreover, to adapt to the changing conditions for continued growth (Rüegg-Stürm and Grand, 2015, p. 78).

The concept of blockchain emerged in 2008 as an innovative technology in the sphere of currencies and payment methods. Initiated by the pseudonymous Satoshi Nakamoto (2008, pp. 1f.), the blockchain was a new idea for an electronic cash system based on cryptography resulting in the so-called "cryptocurrencies." The concept aimed at transforming how transactions were conducted, leading to fundamental changes in the financial system and influencing its structures behind. After the financial crisis of 2008, the related loss of confidence in the prevailing financial system, and recent discussions of the International Monetary Fund (IMF) about the elimination of hard cash (IMF, 2017, pp. 4f.; Papadopoulos, 2015, p. 160), the cryptocurrencies have caught the attention of innumerable individuals, companies, and entire nations.

There are several kinds of cryptocurrencies, and currently, the most famous and widespread is "Bitcoin." The extent and prevalence of the nine-year-old cryptocurrency can be demonstrated by its considerable market cap, which was approx. USD 148 bn. as of February 4, 2018 (Coinmarketcap, 2018, 20. January). According to recent statistics of the Central Intelligence Agency (2018), this is equivalent to the actual stock of narrow money (M1) of countries such as Venezuela and Finland.

In general, Bitcoin can be used as medium of exchange or as a storage of value, i.e., as an investment (de Jong, 2015, p. 416). Some retailers already accept Bitcoin as an additional

DOI: https://doi.org/10.5282/jums/v4i2pp195-227

payment method to purchase their goods and services. The most frequently mentioned advantages of digital currencies as a payment method are the speed, the price savings, and the increased security of (global) transactions, without the necessity for neither a customer nor a vendor to be a registered bank client and, moreover, without the involvement of any financial institution in the transaction process (Bank for International Settlement [BIS], 2015, p. 3).

At first glance, this innovation seems impressively progressive, as it is a payment process that is more efficient, has almost no transaction fees, and has fewer intermediaries. However, the novelty of the technology also introduces uncertainty and unfamiliar risk factors for the participants of the system. Consequently, the enterprise risk management (ERM), particularly of companies and retailers accepting cryptocurrencies as a payment method, will face new challenges.

Due to a lack of research on the appropriate handling of cryptocurrencies in business operations, this thesis aims at developing a holistic framework that supports companies accepting cryptocurrencies in establishing an appropriate risk management system for dealing with cryptocurrencies. Therefore, the following research questions will be addressed:

- What are the potential risks and resulting threats of accepting cryptocurrencies as a payment method?
- Are the companies and the responsible employees aware of these risks, and how do they evaluate and address them?
- Are there any general control activities and recommendations necessary to ensure an appropriate risk management in the handling of cryptocurrencies?

1.2. Structure

This paper has been structured as follows: The introduction (Chapter 1) emphasizes the relevance of the topic, the lack of research, and presents the research questions that will be addressed in order to examine the influence of cryptocurrencies on risk management by the example of Bitcoin. Subsequently, Chapter 2 presents an intensive literature review on the topic of cryptocurrencies and ERM. Chapter 3 presents the research approach adopted, which clarifies the research concept and the methodology employed. On this basis, the results containing the empirical investigation follow in Chapter 4, which is divided into three linked sub-sections, one for each of the three research questions. After the theoretical risk identification process, the aspects of practical risk awareness and risk handling will be analyzed. Based on the obtained insights and results, the author provides general recommendations in the form of a risk control matrix and establishes a holistic Cryptocurrency IC Framework. Finally, the conclusion in Chapter 5 summarizes and discusses this study and identifies its limitations.

1.3. Empirical Approach

The empirical approach employed to investigate the research questions was an online survey sent to a predetermined group of companies accepting Bitcoin payments. Because of the small number of companies currently accepting Bitcoin payments in Switzerland, the selection process of the sample was not limited by any particular industry or geographical region within Europe.

The survey contains qualitative and quantitative questions about the Bitcoin transaction process, Bitcoin administration and the awareness as well as the evaluation of risk factors arising from the use of cryptocurrencies. Further, companies were also asked about the internal controls implemented, if any, for their operational dealing of cryptocurrencies.

The evaluation of the survey responses will be conducted in a descriptive manner. In this context, qualitative questions will be assessed using the concept of inductive content analysis, whereas quantitative questions will be evaluated using nominal, ordinal and interval scales.

2. Literature Review

2.1. Cryptocurrencies

> "There are 3 eras of currency: commodity based, politically based and now, math based."
> Chris Dixon, 2015

2.1.1. Taxonomy

The story of forms of money can be traced back to the early ages of mankind when people traded goods for valuable commodities, such as seashells or cattle. Over time, several other kinds of payment instruments emerged like metals or coins, all of which were linked to their intrinsic value, depending on their weight and purity. (Dombrowski, 2014, p. 9f.)

The introduction of paper money simplified the handling and exchange of money, making transactions more convenient. The value of the paper could be derived in various ways, e.g., by pegging it to a scarce commodity like gold (the former "gold standard") or what is commonly known as "fiat money." The value of fiat money, such as the US Dollar, the British Pound, or the European Euro is determined by "the demand and supply of the nation's currency and its acceptance is enforced by the government through such means as declaring it legal tender" (Dombrowski, 2014, p. 12). This implies that its value depends on factors such as social convention or future expectations of economic developments (Franco, 2014, pp. 4-5).

According to Nian and Chuen (2015, pp. 7-8), "there are various socioeconomic forces that drive the demand for alternative currencies," such as political instability, technological progress, or inefficiencies. An accumulation of these factors might lead to dissatisfaction and consequently to a loss of trust in national currencies and the financial system

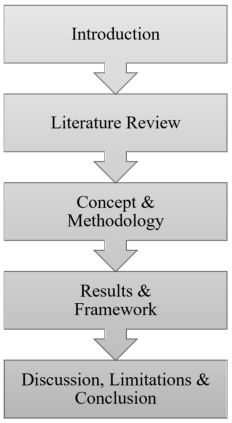


Figure 1: Structure of this Thesis; Source: Own illustration

Table 1: Comparison of Various Types of Currency; Source: Own illustration according to Greene and Shy (2014, p. 275)

	Physical	Digital
Government backed	Cash	E-Cash
Not government backed	Private Money	Virtual Currency

as a whole. A prime example of this was the financial crisis of 2008. In order to establish an independent system that aims at tackling the above-mentioned causes for the demand of alternative currencies and the related discontent, Satoshi Nakamoto (2008, p. 1) proposed the concept of the first decentralized digital currency in a whitepaper entitled, "Bitcoin: A Peer-to-Peer Electronic Cash System."

Table 1 presents a classification of digital currencies as proposed by Greene and Shy (2014, p. 275).

As can be seen in Table 1, there is a general distinction between physical and digital currency. Additionally, there is a differentiation between currency that is or is not government backed. According to the recent definition of the US Government Accountability Office, "a virtual currency is generally considered as a digital unit of exchange that is not backed by governmental-issued legal tender" (United States Treasury Inspector General for Tax Administration (TIGTA), 2016, p. 1), whereby its "value [is] stored electronically in a device such as a chip card or a hard device in a personal computer" (Bank for International Settlement [BIS], 2015, p. 4). This declaration contradicts the basic property of e-cash, because it represents government-issued money; however, it is even stored in the form of bits on a chip, like a chip card or a mobile device (Green & Shy, 2014, p. 275).

To better understand a digital cryptocurrency and its structure, it is important to keep in mind that a digital currency (or "virtual currency" as it is also known) describes the "umbrella term," whereas "cryptocurrency" solely represents a subset with specialized properties (Nian and Chuen, 2015, p. 6). For instance, airline miles or tokens for online games can be classified as digital currencies as well (Nian & Lee Kuo Chuen, p. 8). Figure 2, reproduced from the IMF (2016, p. 8), presents an accurate taxonomy of virtual currencies.

Figure 2 can be summarized as follows: A cryptocurrency

- has no legal tender
- is a medium of exchange for "real-world" items or "real-world" money
- has no central authority that controls and regulates the money circulation
- uses mathematics, particularly cryptography, to validate transactions.

Using the example of Bitcoin and its blockchain, the following chapters will present an in-depth explanation of the structure and application of Bitcoin as a payment method.

2.1.2. Bitcoin

We begin this section by pointing out the general distinction made between the two forms of this term, which are commonly used in English- and French-speaking areas: "Bitcoin" refers to the network and its technology, while "bitcoin" refers to the unit of currency (Gisler, 2015, pp. 9-10).

Concept

The fundamental idea of Bitcoin is derived from the white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System," written by the pseudonymous Satoshi Nakamoto in 2008. This paper illustrated the idea of a purely peer-to-peer (P2P) version of electronic cash without the involvement of any financial third parties (Nakamoto, 2008, p. 1). Bitcoin became the first decentralized digital currency, which implies that there is neither a person nor an institution who is backing, controlling, or regulating the currency (Franco, 2014, pp. 3-4). Instead, Bitcoin "is shared by all network nodes, updated by miners, monitored by everyone, and owned and controlled by no one" (Swan, 2015, p. 1).

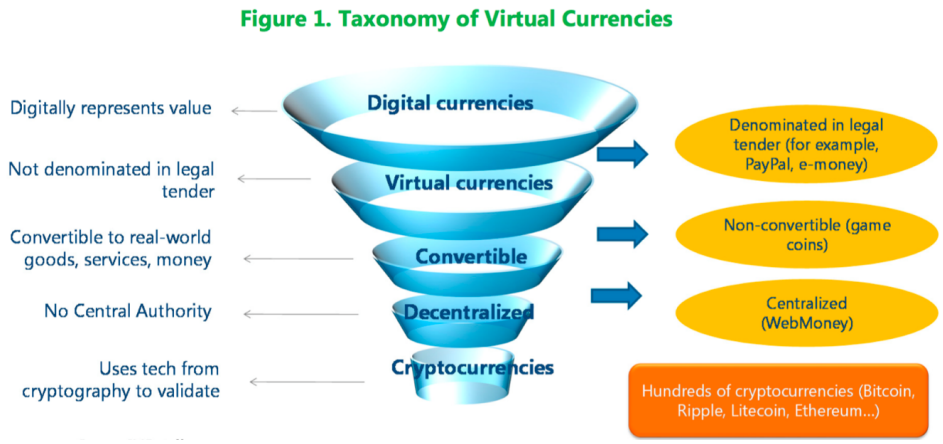


Figure 2: Taxonomy of Virtual Currencies; Source: IMF (2016, p. 8)

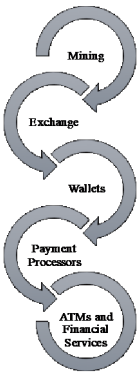


Figure 3: The Bitcoin Value Chain; Source: Own illustration according to Bitcoin Foundation (2017)

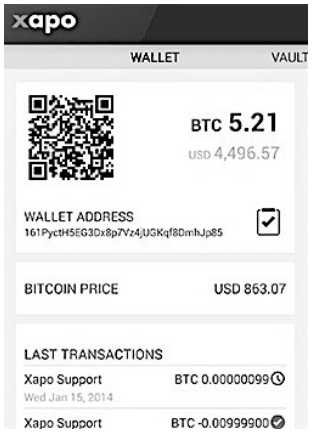


Figure 4: Bitcoin Wallet Screenshot; Source: https://bitcoin.org/img/screenshots/xapo

Nakamoto (2008, p. 1) presented the idea of "an electronic payment system based on cryptographic proof instead of trust." It aims at tackling the problems associated with a centralized financial system and further protecting buyers and sellers from fraud by means of the irreversibility of transactions as well as a P2P distributed timestamp server structure. Moreover, it creates the possibility of reaching the unbanked population and aims at eliminating the disproportional remittance and exchange fees involved in, especially, small-amount transactions. For instance, when sending money to any African countries or when supporting any micro-financing projects, the remittance bears the risk of the transaction cost being higher than the amount originally transferred (Nian and Chuen, 2015, pp. 13-23). Additionally, the proposed approach tackles the so far unsolved double-spending problem in a distributed financial database without the necessity of an intermediary who charges (high) transaction fees for the validation, such as banks, credit card

companies, or other established payment transmitters like PayPal (Deloitte, 2016, p. 5; Franco, 2014, p. 6; Papadopoulos, 2015, p. 158).

According to Papadopoulos (2015, p. 155), bitcoins are the digital equivalent of cash, which is designed to transfer "economic value across the internet." Basically, the concept of Bitcoin can be compared with mining gold, whereby the globally available amount of gold would be equal to the limited availability of bitcoins (Tindell, 2013, 5. March). To further explain this comparison, the bitcoin "creation process" – the so-called "mining" – is conducted by a decentralized P2P network of computers working around the clock to solve difficult mathematical problems based on cryptographic hash algorithms instead of gold miners physically digging for gold (Antonopoulos, 2015, p. 175; Cusumano, 2014, p. 22).

When a mathematical problem is solved, the successful miner(s) are rewarded in the form of bitcoins for providing their processing power and the necessary energy. Finally, the earned as well as the previously spent bitcoins are stored "in a notional ledger held across many computers around the world" (the blockchain) and not in underground vaults as in the case of gold bars (Tindell, 2013, 5. March).

The Bitcoin Value Chain

As described in the previous section, the bitcoin creation process differs from the issuance of fiat money, whose supply is controlled and regulated by the central bank. In comparison, in the Bitcoin ecosystem, the blockchain, which is based on a P2P network of computers executing a determined algorithm (the Bitcoin protocol), takes charge of this responsibility. This implies two core properties of Bitcoin: first, there is no centralized regulatory instance that is responsible for these tasks, and, second, the supply of money is limited to 21 million bitcoins because of one (of many) requirements determined by the Bitcoin protocol (Bhaskar and Chuen, 2015, p. 53). Additionally, the mining process is defined through a predictable progressive growth rate, which will converge toward zero until the year 2140. Hence, the issuance as well as the mining rewards will be halved approx. every four years which is equivalent to every 210,000 blocks mined (Bhaskar and Chuen, 2015, p. 53).

In 2009, the first bitcoin was mined and as of January 20, 2018, approx. 16.8 million bitcoins have been issued, which is roughly 80% of all the potentially available bitcoins (Coindesk, 2018, 20. January). When the newly emerged bitcoins are mined, they are first added to the blockchain and, subsequently, attributed to the successful miner(s). A miner has two options: on the one hand, he has the possibility to sell the bitcoins against fiat currencies or other cryptocurrencies on a specific cryptocurrency exchange platform like bitfinex.com or bittrex.com. On the other hand, the rewarded bitcoins can be transferred directly to his wallet and can thus be used for personal purposes, e.g., as a medium of exchange for real or digital goods and services or as an investment (de Jong, 2015, pp. 416-417). An overview of the Bitcoin value chain can be found in Figure 3.

In order to use and store bitcoins, regardless of how the bitcoins are received – as a mining reward or bought on an exchange platform – one has to download a so-called "wallet." A wallet is an application, typically for smartphones, tablets, or desktop computers, through which an owner of bitcoins is able to store, send and receive Bitcoin funds (Bitcoin Foundation, 2017). Moreover, a wallet runs a key generation software that creates a public address (known as a wallet address) and stores the corresponding private key (Franco, 2014, p. 56). In this context, wallets are often described as "containers for private keys," because the bitcoins themselves are stored on the blockchain and not in the user's wallet, i.e., a wallet keeps only the corresponding private key to sign a transaction and transfer the property rights of a bitcoin (Antonopoulos, 2015, p. 86). More information about the transaction process is given in Section 2.1.3.2. A wallet application also enables the conversion of public addresses to QR codes, the management of incoming and outgoing payments, and displays the currently available funds (Sixt, 2017, p. 37). A screenshot of a wallet can be seen in Figure 4.

As described, Bitcoin payments can be sent or received by means of a wallet application. Therefore, the sender has to type in the public address (or scan the QR code) of the recipient and specify the number of bitcoins that should be debited from the account.

In order to simplify the implementation of Bitcoin acceptance, to overcome the general complexity of the technological novice, and the "bottlenecks in exchanging" into fiat currencies, merchants often use a payment processor (Papadopoulos, 2015, p. 161). This is a company that serves as a third-party provider and offers services for retailers to handle their payments by providing a technical infrastructure such as payment terminals, mobile apps, or e-commerce plugins. These tools are commonly able to quote prices in the national currency, directly convert bitcoins into the national currency, and instantly confirm the transactions and thus ensure that there is no risk of a payment default. All of this is done in exchange for a transaction fee amounting to 0.5-1% of the invoiced amount. This is cheaper than using credit cards whose fees are 2-3% per transaction. (Cusumano, 2014, p. 23; Franco, 2014, p. 43)

At the end of the Bitcoin value chain, there are the several applications of Bitcoin, which are mainly based in the payment and investment industry, for instance, making purchases, holding it as an investment asset, or making further investments in other currencies or decentralized autonomous organizations (DAOs). Due to the increasing acceptance but continued lack of know-how about the complicated procedures behind the entire value chain, Bitcoin-interested parties are also able to instantly exchange their (fiat) money in bitcoins more conveniently by way of a Bitcoin teller machine (BTM). They can then later transfer them to their wallet and are thus finally able to participate in the Bitcoin application universe (Cohen, 2014, pp. 18-19).

Merchant Acceptance & Market Capitalization

At the time of writing this thesis, there are more than 1500 established cryptocurrencies (cf. Worldcoinindex, 2018, 9.

February). According to Elfriede Sixt (2017, pp. 111f.), the alternatives to Bitcoin are called "altcoins," which differ in several ways, but primarily in terms of the underlying technological structure (blockchain and protocol), which influences the validation process, the money supply, and the purpose of the digital token issued (currency, smart contract, investment token, usage token, utility token, etc.).

In the recent years, an increasing number of merchants have started to accept Bitcoin payments. The payment processor Coinbase's advertisements state that "over 48,000 merchants" use its technical infrastructure to accept Bitcoin payments. This includes multinational companies from several industries, such as the online retailer overstock.com, the IT company Dell, and the online travel company Expedia (Coinbase, 2018, 12. February). Moreover, there are at least ten payment processors, apart from companies that do not use any payment processor. Unfortunately, there is no global unambiguous number of merchants who actually accept Bitcoin payments. For instance, the platform coinmap.org (optional registration platform for Bitcoin merchants) lists approx. 11,400 merchants who accept Bitcoin payments as on January 5, 2018 (Coinmap, 2018, 5. January).

In fact, as of January 20, 2018, Bitcoin had a total market cap of USD 214.2 bn., which is equivalent to 34.8% of the entire crypto market cap. Further, about 315,000 Bitcoin transactions had been conducted in the previous 24 hours (Blockchain, 2018, 20. January; Coinmarketcap, 2018, 4. February) – six times more than four years ago. Moreover, one bitcoin has a value of around USD 12,600 (Coinmarketcap, 2018, 4. February), which has increased by approx. 1400% during the last year.

2.1.3. Blockchain

In recent times, blockchain technology has attracted more and more industries. The application of the technology goes far beyond the scope of cryptocurrencies. Massimo Di Pierro (2017, p. 92), professor at the School of Computing of DePaul University, states that the problems of authentication, integrity, and non-repudiation are solved by this disruptive technology because it deals with the "problem of creating a distributed storage of timestamped documents where no party can tamper with the content of the data or the timestamps without detection."

The decentralized database system enables the emergence of new use cases due to its ability to assign things to identities in a tamper-proof and decentralized manner, such as a decentralized notary, e.g., the attribution of physical goods like real estate, gold, or diamonds to digital identities (Deloitte, 2016, p. 5). Particularly, in the world of intellectual property, the double-spending issue represents a huge problem because of the "copy and paste" possibilities. Based on the fact that there is no database documenting the purchase/sale of a digital token (such as a song, for example), the token can be shared in an unlimited manner (Vigna and Casey, 2016, p. 120).

This vulnerability of double-spending can be eliminated by means of the decentralized consensus process of the Bitcoin blockchain (Underwood, 2016, p. 15). In general, "a double-spend attempt occurs when a user tries to spend some funds twice," which plays especially a significant role in the financial system because all financial institutions must reject these attempts (Franco, 2014, p. 6). In a centralized system, this "is relatively straightforward [...] because transactions are recorded in a central database and future spending attempts are checked against this database first" (Franco, 2014, p. 6). Controversially, in a "decentralized system, many copies of the database are shared among the peers, and keeping a consistent state of the database is a difficult computational problem" (Franco, 2014, p. 6).

According to Antonopoulos (2015, p. 3), the Bitcoin network exhibits, by means of its underlying technology (the blockchain), four key innovations functioning in a "unique and powerful combination":

- A decentralized mathematical and deterministic currency issuance (Mining)
- A decentralized P2P network
- A decentralized transaction verification system
- A public transaction ledger

In order to explain these innovations, this chapter is divided into three subsections: Structure, Transactions Process, and the Decentralized Consensus of a Transaction (Mining).

Structure

The blockchain is the underlying technology that operates a cryptocurrency and thus represents the fundamental prerequisite for its existence. Cryptocurrency experts like Vigna and Casey (2016, p. 120) describe the Bitcoin blockchain as "bitcoin's central nervous system." Some confusion might arise from the fact that the term Bitcoin is used for all three layers in the technology stack of the Bitcoin blockchain, i.e., "Bitcoin" refers to the blockchain, its protocol, as well as the available currency and tokens issued (Franco, 2014, pp. 18-19). However, Figure 5 presents a general link between these three layers.

The Bitcoin blockchain is essentially a database that is represented by its nodes and "replicated as many times as there are nodes" (Morettini, n.D.). These nodes provide their central processing unit (CPU) to the Bitcoin network to run a software known as the Bitcoin protocol. This is why Morettini (n.D.) states that the Bitcoin blockchain can even be described as a "supercomputer formed by the combination of the CPUs [...] of all its nodes." In this context, it is important to understand that the Bitcoin blockchain is not a tool for the transmission of bitcoins; it is rather "an authoritative public record that records the chain of title for any current bitcoin holdings" (Lloyds, 2015, p. 7). This implies that from a technical point of view, a blockchain is a database allowing data collection in the form of data packages which can be easily accessed, updated, and managed (Rouse, 2017).

From an application-oriented, comparable, and conceivable view, the Bitcoin blockchain is often considered as a

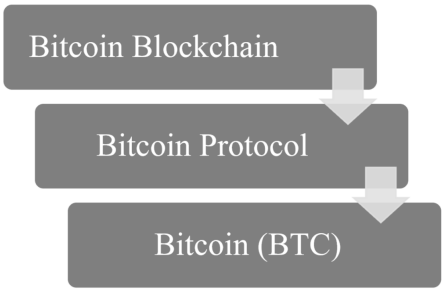


Figure 5: Layers in the Bitcoin Blockchain Technology Stack; Source: Own illustration according to Swan (2015, p. 1)

"general ledger," because each transaction that has ever been conducted since January 3, 2009, is recorded in this publicly accessible and non-reversible transaction ledger (Sixt, 2017, p. 30; Franco, 2014, p. 95). In general, a blockchain can be compared with an endless table containing three columns: the transaction's timestamp, the transaction's details, and the corresponding hash (Di Pierro, 2017, p. 93).

The Bitcoin protocol, which is executed by the nodes, takes charge of the proof and verification process of transactions determined in a decentralized consensus process (Vigna and Casey, 2016, p. 124). The underlying software algorithm (the Bitcoin protocol) determines the steps that any node has to execute in order to accomplish a general consensus for a transaction, i.e., either to validate and confirm or to deny a transaction (Sixt, 2017, pp. 1-2). Additionally, the protocol defines the properties of cryptocurrency, such as the (limited) amount of coins issued or the explicit details (halving time, coins per block, etc.) about the (deterministic) coin issuance. In general, it can be stated that the Bitcoin protocol sets the rules and the framework conditions for a cryptocurrency.

Thus the existence of a cryptocurrency token (such as one bitcoin) can be attributed to a database (the blockchain), which operates the appropriate software (the protocol). Each cryptocurrency consists of at least these three layers (Swan, 2015, p. 1).

Transaction Process

The transaction process can be generally divided into two steps: the authorization process by means of digital signatures and a decentralized verification and validation process (mining).

A bitcoin is a unique number that results as the solution of a cryptographic puzzle (Di Pierro, 2017, p. 93). Thus, a transaction is the change of ownership of this number, which in turn requires the authorization of possessing and transferring this number, i.e., a single bitcoin or its fractions (Antonopoulos, 2015, p. 18). However, the question is how a transaction works and, in turn, how the ownership of a bitcoin changes. Bitcoin's inventor Satoshi Nakamoto (2008, p. 2) defined an electronic coin as "a chain of digital signatures." Hence, a transfer of the ownership and control of a coin is achieved "by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin" (Nguyen, 2017, p. 1). In this context, the blockchain stores this chain of digital signatures (Lloyds, 2015, p. 7).

This sounds extremely complicated at first glance, but it can be simplified in the following way: In the Bitcoin network, the transfer of bitcoins is authorized and initiated by digitally signing a transaction. This digital signature process is based on a public-private key pair, which is based on its cryptographic origin, or, to be more specific, to the calculation of elliptic curves that are based on the Elliptic Curve Digital Signature Algorithm (ECDSA) (Sixt, 2017, p. 37). Nevertheless, although the public key can be compared with a bank account number, the private key serves as the signature unlocking this bank account (Franco, 2014, p. 56). The possession and control of a bitcoin (or its fractions) is the same as having knowledge about the private key that is mathematically linked to the public address/key (Lloyds, 2015, p. 7).

For instance, let's say a signer called Alice would like to buy a coffee at Bob's café (the recipient). To begin, Alice needs a public-private key pair that is usually automatically generated by her Bitcoin wallet. She then sends her public key to the recipient (2). In the meantime (3), she uses her private key to digitally sign the transaction terms (called a "message" in Figure 6) containing the transaction details (i.e., price and terms) along with a timestamp (Di Pierro, 2017, p. 93; Goldman Sachs, 2016, pp. 8f.). When the transaction is transmitted (4) to Bob, he is able to verify it using Alice's public key (5). If the verification goes through, he knows that Alice has triggered the payment and that she has transferred her ownership rights of the bitcoins to him (6). An overview of this digital signature process can be seen in Figure 6 above. In practice, these "technical" steps are not conducted by Alice or Bob but by their wallet applications, which are linked to the Bitcoin protocol. Finally, the signatures are proofed and verified by the nodes of the Bitcoin blockchain (Franco, 2014, pp. 56-57).

To sum up, a digital signature serves two purposes: "(1) to verify the transaction to be sent and validated to the Bitcoin network, and also (2) to confirm her assent to the transaction" (Nguyen, 2017, p. 2). When a transaction is signed, the verification and validation process begins by generating a computational hash, which is conducted by a decentralized network of miners in a process known as the "mining process", cf. Figure 7.

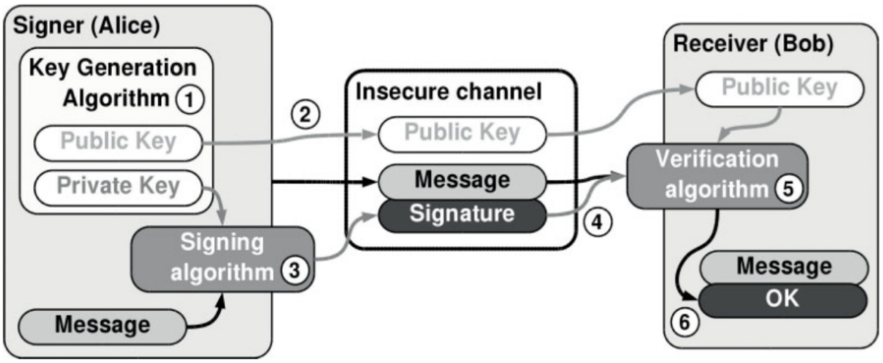


Figure 6: Digital Signature Process; Source: Franco (2014, p. 57)

The Decentralized Consensus of Transaction (Mining)

This mining process is conducted by all network nodes or "miners," who are essentially electronic bookkeepers. In general, Bitcoin transactions are similar to the entries in a double-entry bookkeeping ledger (see Figure 8). On one side, there are the credits on a Bitcoin account (the inputs) resulting from one or more incoming Bitcoin payments or mining earnings. On the other side of the ledger are the debits (the outputs) that equal to the Bitcoin payments made. In this context, the inputs need not to be equal to the outputs, with the difference being the transaction fees for the miners. (Antonopoulos, 2015, pp. 18-19)

When a transaction is signed, it is first shared among the network nodes (Antonopoulos, 2015, p. 25). In order to review and validate the transaction, the miners include all transactions (since the last mined block) to the next block of the blockchain, which has to be subsequently mined. Now the mining process begins: Mining is based on a cryptographic concept where nonces are randomly guessed, until the right one is found – the so-called "proof-of-work" (Sixt, 2017, p. 40). The nonce is a random number used for the verification of a unique hash calculated using cryptographic means (Nofer et al., 2017, pp. 183-184).

From a more comprehensive view, Bitcoin mining can be described as a competitive Sudoku "that resets every time someone finds a solution and whose difficulty automatically adjusts so that it takes approx. ten minutes to find a solution" (Antonopoulos, 2015, p. 26). The successful miner who solves the Sudoku (or the algorithm) and finds the proof-of-work, shares this solution with the other network nodes. The other miners verify the result and, subsequently, propagate the new block in the network (Antonopoulos, 2015, p. 26).

If this new block is validated, it will be "sealed" and recorded in the blockchain while the miners go on to solve the algorithm of the next block (Antonopoulos, 2015, p. 27). Furthermore, the timestamp and the nonce are added to the mined block and thus a blockchain can be compared with a table containing three columns: the transaction's timestamp, the transaction's details, and the corresponding hash (Di Pierro, 2017, p. 93). In order to make this database tamper-proof, the hash of the previous block is included as well. Therefore, it is not possible to change any transactions that have already been conducted, verified and confirmed without changing the entire blockchain, because any change would immediately affect the hash values calculated (Nofer et al., 2017, pp. 183-184). This implies that no one can counterfeit the blockchain without the network noticing it, because each peer keeps a copy of the entire common asset ledger (Franco, 2014, p. 8; Morettini, n.D.). Figure 9 provides an overview of an example of a blockchain.

Referring again to our previous example, Alice gets her first payment confirmation after the block containing her transaction is sealed. If the next block is mined, Alice will get her second confirmation and so on. This implies that each block mined on top of the block containing the initial transaction represents an implicit confirmation and thus it will be exponentially harder to reverse or manipulate a transaction. Usually, a block with more than six confirmations is considered as "irrevocable" because it would cost an extremely large amount of computational power to recalculate six blocks (Antonopoulos, 2015, p. 28).

As already described, the miners provide their computers' power (CPUs) to the Bitcoin network in order to execute the Bitcoin protocol, which determines the steps a computer has to execute to validate or deny a transaction to the blockchain (Böhme et al., 2015, p. 215; de Jong, 2015, p. 417). In exchange for providing their processing power, the miners get paid for their "work" through incentives or "mining rewards," which is in the form of newly issued bitcoins (Gisler, 2015, pp. 13-14). Every ten minutes, new bitcoins are issued due to the period of the validation process (Vigna and Casey, 2016, p. 132). See Figure 10 that outlines this entire process.

The new issuance of bitcoins therefore occurs six times per hour and 144 times per day, or, in other words, 144 blocks are mined per day. Due to the fact that the mining rewards are halved every four years, cryptocurrency experts like Antonopoulos (2015, p. 3) speak about a "deterministic currency issuance" in case of Bitcoin. Currently, there are approx. 500,000 mined blocks and the mining reward per block is about 12.5 bitcoins (Blockchain, 2018, 20. January).

In summary, it can be stated that the mining process fulfills two interrelated core tasks: on the one hand, the is-

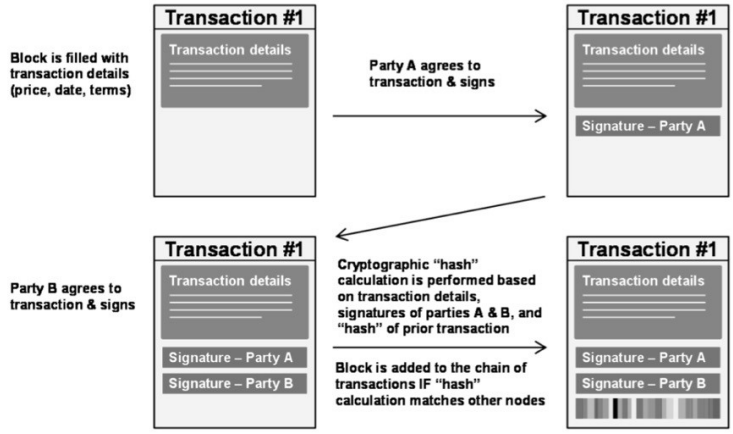


Figure 7: Transaction Process; Source: Goldman Sachs (2016, p. 8)

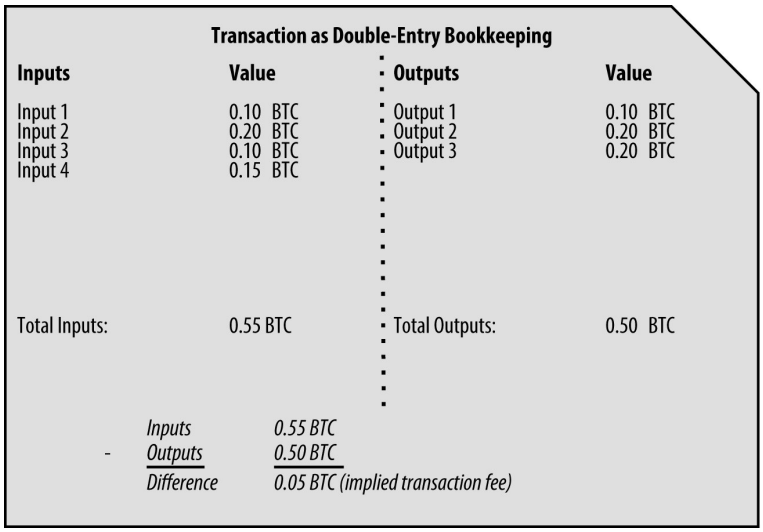


Figure 8: Transaction as Doubly-Entry Bookkeeping; Source: Antonopoulos (2015, p. 19)

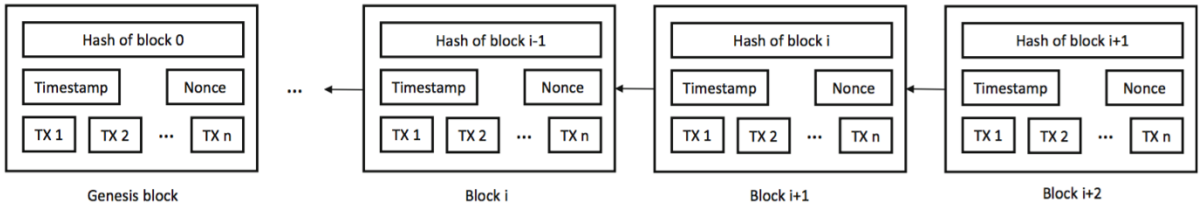


Figure 9: Example of a Blockchain; Source: Nofer et al. (2017, p. 184)

suance of new bitcoins, which is quite similar to a central bank printing new money, and, on the other hand, the validation of transactions, which is its main purpose (Antonopoulos, 2015, pp. 25; 175-176). An overview of the entire mining process can be found in Appendix 1 – The Mining Process.

2.1.4. Regulation

Notwithstanding, Bitcoin has gained popularity no just as a form of currency in the context of e-commerce. Particularly in consideration of regulatory issues, cryptocurrencies have in the meantime caught the attention of countries and communities of states as well. The increasing market capitalization and discussions about the classification of virtual currencies have fostered the consideration of virtual currencies as a subject of regulation; for instance, in April 2017, Japan announced that it officially recognizes Bitcoin as a legal tender (Gautham, 2017). In comparison, there are also countries such as Bolivia, Vietnam, and Bangladesh that have completely banned Bitcoin and declared cryptocurrencies as illegal (Swan, 2015, p. 7).

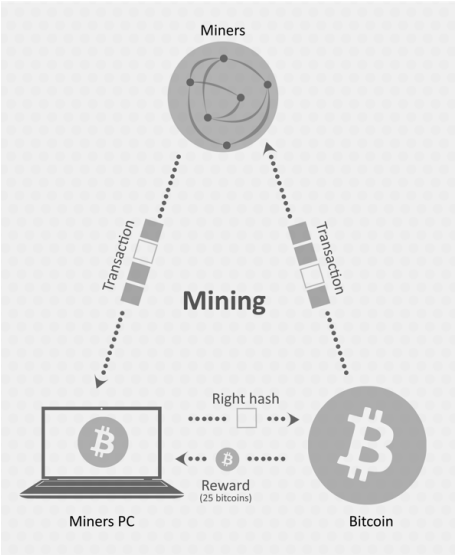


Figure 10: The Bitcoin Mining; Source: http://en.bitcoinwiki.org/Mining

In 2012, the European Central Bank (ECB, 2012, p. 13) classified Bitcoin as a virtual currency with the following definition: "A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." Until now, Bitcoin is still not specifically regulated in the European Union (EU) including Switzerland (Piller, 2017, p. 9); however, in recent weeks, there have been many proposals to consider virtual currencies at least in the national regulations around Anti-Money-Laundering (AML) and Know-Your-Customer (KYC) issues (Kollewe, 2017, 4. December). This is perhaps mainly due to the significant price development (cf. Appendix 2) and the remarkable market capitalization during the last year. Therefore, a greater number of voices are now demanding a stronger regulation of Bitcoin, especially in consideration of money laundering issues (Berschens et al., 2017, 19. December; Kollewe, 2017, 4. December).

2.2. Enterprise Risk Management & Internal Control

2.2.1. Definitions & Relevance

Risks are dynamic, fluid, and extremely interdependent (Lam, 2014, p. 51). In today's highly volatile and dynamic environment, a company requires an integrative approach to manage its risk portfolio instead of single detective controls that are implemented and monitored by separate business units (Lam, 2014, p. 51). For instance, the implementation of a new payment method, such as the acceptance of cryptocurrencies, does not solely influence the accounting and controlling department as an additional payment option that has to be considered in the revenue recognition and consolidation. There might even be some fundamental adaptions due to emerging risks in the underlying IT infrastructure/security, operational dealings, as well as the compliance of new regulations by accepting these payments. Therefore, an integrative approach across several business units is required.

The ERM function takes charge of this responsibility by establishing "firm-wide policies and standards, [coordinating] risk management activities across business units and functions, and [providing] overall risk monitoring for senior management and the board" (Lam, 2014, p. 51). The objective of ERM is to ensure that the company's management is able to effectively deal with uncertainty and its associated risks. In order to achieve this, the approach aims at ensuring the effective running of business operations, accurate reporting and compliance with regulations to prevent any events that might damage the company's reputation (COSO, 2004, p. 1).

The concept of internal control (IC) is an integral part of an entity's risk management. In general, IC is defined as "a process, effected by an entity's board of directors (BoD), management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" (COSO, 2013, p. 3). This implies that IC does not only describe the detective and the corrective controls associated, it also proposes an integrative approach including directive and preventive controls to ensure that no misconduct or adverse event can occur that might negatively affect the company's objectives (Ruud and Jenal, 2005, p. 456).

For this purpose, the implementation of the COSO IC Framework provides a proper method of solution, established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This risk management framework outlines components, principles, and factors that are necessary to effectively manage risks (COSO, 2015, p. 1). However, "although risk management frameworks can effectively identify the types of risks that modern businesses must control, these frameworks are largely silent about how specific duties should be assigned and coordinated within the orga-

nization" (of Internal Auditors , IIA, p. 1). Therefore, the proper assignment of duties and responsibilities related to IC within an organization's governance is a prerequisite. In this context, the Three Lines of Defense (TLoD) model provides a simple and systematic approach to improve the effectiveness of a company's risk management (of Internal Auditors , IIA, p. 2).

2.2.2. Internal Control

In an Organization's Governance

By describing IC's responsibilities and further differentiating it from the internal audit function within a corporation, the TLoD model, established by the European Confederation of Institutes of Internal Auditing (IIA) and the Federation of European Risk Management Associations, is being increasingly used and generally accepted as an institutional framework (Casari, 2017, p. 17; Hunziker, 2015, p. 52). This framework is employed to address "how specific duties related to risk and control could be assigned and coordinated within an organization" with the objective of increasing the likelihood of achieving the company's objectives (COSO, 2015, p. 1). It can be seen as a set of guidelines for how risk and control duties must be allocated and executed within an organizational structure. Moreover, such effective coordination of responsibilities prevents a duplication of efforts and controls, which in turn fosters a more effective risk management approach (of Internal Auditors , IIA, p. 1).

The TLoD model is based on the assumption that "three lines" within an organization are necessary for the effective management of risk and control (cf. Figure 11):

- 1st Line of Defense: Operating management that is responsible for owning and managing risk and control
- 2nd Line of Defense: Management support that takes care of monitoring the risk and control
- 3rd Line of Defense: Independent assurance concerning the management of risk and control

As can be seen in Figure 11, the senior management and the BoD as well as external parties such as the external auditors or regulators play integral roles (Hunziker, 2015, pp. 52-53). Whereas the senior management is responsible for selecting, developing, and evaluating the IC system, the BoD will manage and overview the entire process (COSO, 2015, p. 4). Both groups are primary stakeholders, served by the three lines. It is their "responsibility and accountability for setting the organization's objectives, defining strategies to achieve those objectives, and establishing governance structures and processes to best manage the risks in accomplishing those objectives" (of Internal Auditors , IIA, p. 3). Additionally, they are in the best position to help ensure and actively support the implementation of the TLoD (of Internal Auditors , IIA, pp. 2-3).

External auditors, regulators, and other external parties are outside the organization's structure. Even still, they are able to influence the organization's government and control structure, e.g., by setting requirements to strengthen the control or by performing independent assessments. This implies that an external body can become an additional line of defense by "providing assurance to the organization's shareholders, including the governing body and senior management." (of Internal Auditors , IIA, p. 6)

To sum up, the TLoD framework can be described as a prerequisite but also as a complimentary framework to the COSO IC Framework in order to assign and allocate duties within an organization and to thus ensure proper risk management.

COSO Internal Control – Integrated Framework

In 1992, the COSO issued a report presenting the first COSO IC Framework (Arwinge, 2012, p. 37). In general, the US-based organization is dedicated to improving a companies' financial reporting quality, IC and Corporate Governance (Arwinge, 2012, p. 37). Over time, the COSO has developed and further modified several frameworks that concretize ERM and IC (Graham, 2015, p. 2). These frameworks outline components, principles, and factors that are necessary to effectively manage risks. Moreover, they provide evaluation tools for an organization to assess its IC (COSO, 2015, p. 1; Graham, 2015, p. 2) and therefore represents a worthwhile tool for "directors, managers, auditors, regulators, investors and other concerned stakeholders" (Arwinge, 2012, p. 37).

In the literature on this subject, there is some confusion about the COSO IC and the COSO ERM Frameworks, because the COSO has also published a COSO ERM Framework in 2004. This framework explicitly addresses control mechanisms for the achievement of strategic goals, which thus additionally provide "a more robust and extensive focus on the broader subject of enterprise risk management" (COSO, 2004, p. 5; Hunziker, 2015, p. 36). This implies that the ERM framework intends to expand the initial COSO IC Framework and to establish a more comprehensive framework. However, Buber and Holzmüller (2009, p. 106) states that the ERM and IC Frameworks are almost identical. This statement can be further justified by the fact that the COSO ERM Framework already encompasses the COSO IC Framework. According to the COSO (2013, p. ii) itself, both frameworks are "intended to be complimentary" and they do not supersede each other. For the further analysis, the author focuses on the COSO 2013 IC Framework, shown in Figure 12.

The COSO IC Framework enables "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, p. i).

In order to achieve this, the COSO IC Framework comprises three divisions (see Figure 12): objectives (the three columns), components (the five rows), and organizational structure (the third division). The first and second division are directly related to each other because the entity's objectives – which can be divided into operational, reporting, and compliance categories – require all five components for their

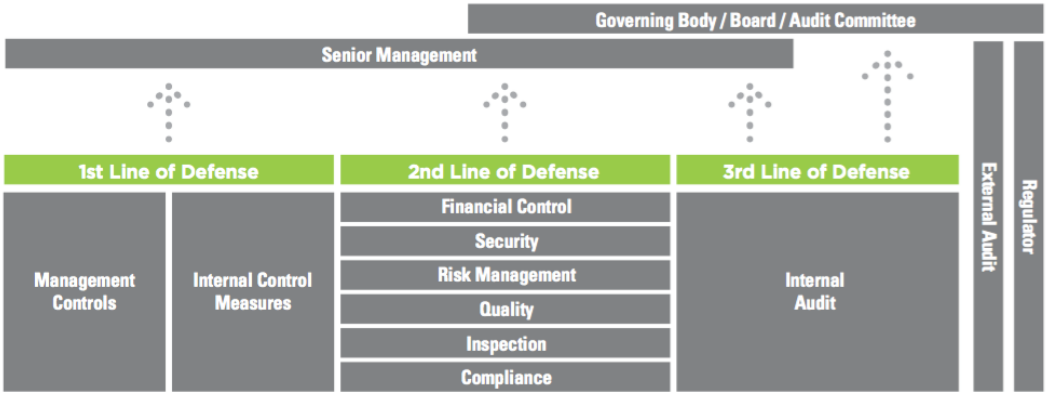


Figure 11: The Three Lines of Defense; Source: COSO (2015, p. 2)

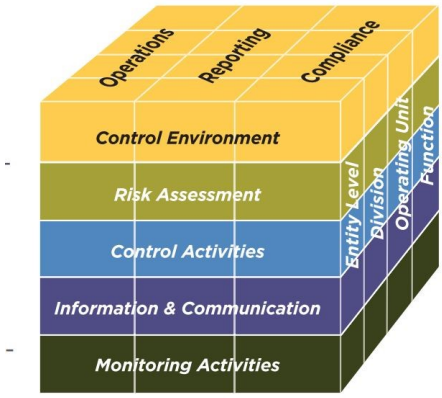


Figure 12: COSO 2013 Internal Control - Integrated Framework; Source: COSO (2013, p. 6)

success. Moreover, IC is relevant to the entire organization (third division), i.e., from the group level to each division, including any business unit and function. (Bungartz, 2017, p. 20; COSO, 2013, p. 6)

The five interrelated key components of IC are: control environment, risk assessment, control activities, information & communication and, monitoring activities (Arwinge, 2012, p. 37; Graham, 2015, p. 2). In a brief summary, they can be described in the following way:

- Control Environment: The control environment defines the basics of the IC within an organization. In this first stage, the "tone at the top" of a company is set when the responsibilities of the BoD and the senior management are negotiated and determined. This has a considerable impact on the working atmosphere within the company, the daily business operations, but also on the handling of risks (Ruud et al., 2008, p. 939). In consideration of factors such as integrity and ethical values and organizational structure and management philosophy, the control environment compromises the establishment of a "sound control environment." This sets the context standards for ethical behavior, corporate culture, and the basis for executing IC across an organization, including the expected standards of conduct (Arwinge, 2012, p. 43).
- Risk Assessment: When the company's objectives and its corresponding control environment are defined, the risks that might negatively affect these can be identified by means of a risk assessment (Ruud et al., 2008, p. 940). Generally, emerging risks can be from internal or external sources. In this context, the risk assessment represents a dynamic and iterative process that evaluates the risks identified according to their likelihood and potential damage (COSO, 2013, p. 4). This process plays an increasingly important role in today's dynamic and fast paced environment and finally provides the basis for decisions concerning how and which risks have to be managed (Bungartz, 2017, p. 39).
- Control Activities: Based on the risk assessment performed, the management decides which control measures (preventive, directive, detective, or corrective) have to be implemented to properly address the risks identified (Hunziker, 2015, p. 32; Pfaff and Ruud, 2013, pp. 73-74). For this decision process, the development of a risk control matrix can be quite useful. According to Pfaff and Ruud (2013, p. 85), a risk control matrix can be employed as tool in order to deal

with, present, and document the risks identified. Table 2 presents a simplified version of a risk control matrix. Depending on the organization's size, the matrix could be more sophisticated to give a more comprehensive understanding of the risks. However, a risk control matrix also enables greater transparency for all involved parties, ranging from employees to external auditors, which improves risk awareness and the appropriate development and adaption of internal controls (Pfaff and Ruud, 2013, p. 86). These implemented control measures may include a range of manual activities like the review of necessary documents as well as automated controls such as software-based journal entry testing. In general, control activities are actions established through policies and procedures "that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out" (COSO, 2013, p. 4). These control activities may be located and further performed throughout the entire organization, i.e., at all levels of the entity and in all business processes (Arwinge, 2012, p. 46).

- Information & Communication: Information obtained from internal or external sources serves as the basis for the communication of internal responsibilities (COSO, 2013, p. 5). In order to ensure that the control activities determined are implemented and effective, the necessary and important information needs to first be identified. Afterwards, this information should be communicated in a comprehensive way, so that it builds the basis for every employee's actions with regard to management and IC in the company (Ruud et al., 2008, p. 940). This implies that information and communication are highly dependent and, moreover, are critical to help achieve a company's objectives (Casari, 2017, p. 23).

- Monitoring Activities: Finally, a company has to assess and ensure the quality of the internal controls implemented over time (Graham, 2015, p. 173), especially given that a company's internal controls have to be continuously adjusted to external and internal changes (Ruud et al., 2008, p. 940). Therefore, the implementation process and the effectiveness of the internal controls require the appropriate monitoring activities to ensure their presence and functioning. These activities may be performed in the form of ongoing evaluations, separate evaluations, or a combination of both (COSO, 2013, p. 5).

In addition to the framework proposed, the COSO has stipulated 17 principles (cf. Appendix 3) aimed at formalizing the above-mentioned concepts "in a more comprehensive manner" (Caserni, 2017, p. 23). These principles have been directly derived from the five key components, and, according to COSO (2013, p. 6), effective IC can be achieved through their implementation and application.

A Regulatory Perspective

The COSO IC Framework represents a key conceptual and practical framework for several groups of stakeholders (Arwinge, 2012, p. 39). Specifically in relation to the emerging issues around Corporate Governance, the framework becomes increasingly important because it serves the fundamental principles (Hunziker, 2015, p. 34). Even though there is no obligation to design and implement IC within an organization, there is certainly a tendency toward stronger regulations (Ruud and Jenal, 2005, p. 455). According to Hunziker (2015, p. 39), this phenomenon is an implication of the negative developments of economies and the several corporate scandals in recent times, such as the Enron or the Dotcom scandal.

The US can be cited as a model example in the context of more stringent regulations. Following the implementation of the Sarbanes-Oxley Act (SOX) in 2002, an organization's management is responsible for IC and has to make a statement with regard to the appropriateness of internal control over financial reporting (ICOFR) (Ruud and Jenal, 2005, p. 455). Additionally, SOX Section 404 prescribes that the financial statement auditor "must assess and report on both management's assessment of the ICOFR and the operating effectiveness on the ICOFR" (Arwinge, 2012, p. 65). The SOX regulation applies to all companies, including foreign subsidiaries, which are listed by the US Securities and Exchange Commission (Caserni, 2017, p. 27; Westerhausen, 2005, pp. 100-101). Therefore, IC represents an integral part of the US' mandatory law and, moreover, needs attestation by an auditor.

In order to improve the Corporate Governance in the EU, its commission also adopted similar guidelines in 2006. The new guidelines bear some similarities to the SOX and aim at harmonizing the regulation of IC across Europe. However, because there are no further European regulations, the respective national laws are applicable (Hunziker, 2015, p. 43). For instance, in Switzerland, the Swiss Code of Obligations (CO) further specifies the role of IC. According to art. 728a, paragraph 1 cipher 3 CO & art. 727, paragraph 1 CO, the external auditor has the duty of examining whether "there is an internal system of control," with all public companies as well as any economically significant company being subject bound by these regulations (Ruud et al., 2008, p. 938). Moreover, the CO states that the BoD has the "non-transferable and inalienable duties" of the company's management and organization, which inter alia includes the organization "of the accounting, financial control and financial planning systems as required for management of the company" (art. 716a, paragraph 1 ciphers 1–3 CO). While the CO only mentions the existence of IC, the Swiss Code of Best Practice for Corporate Governance outlines further recommendations with regard to IC (Ruud and Jenal, 2005, p. 455). However, there are still no legally binding requirements only recommendations concerning IC design and implementation in the EU.

Table 2: Simplified Version of a Risk Control Matrix; Source: Own illustration according to Pfaff and Ruud (2013, p. 85)

Objectives	Risks	Control Activities
...	...	...

2.2.3. Failures and Limitations

Although the implementation of the COSO IC Framework enhances the likelihood of achieving the entity's objectives, one has to keep in mind that IC gives only a reasonable and not absolute assurance (Graham, 2015, p. 15). For instance, a bad judgment made on the basis of a simple error or bias or an external event might negatively affect an entity's operational goals, which cannot be prevented by IC. To sum up, even an effective IC can experience failure due to the following reasons:

- Human error: If the people who have implemented and executed IC make errors, which, in turn, lead to control failures
- Management overrides: A manager is able to override IC control for selfish purposes
- Collusion: The ability to circumvent IC by means of secret agreements (COSO, 2013, p. 9, Graham, 2015, pp. 15-16; Ruud and Jenal, 2005, p. 456)

Hence, an organization's management should be aware of these vulnerabilities "when selecting, developing, and deploying controls that minimize, to the extent practical, these limitations" (COSO, 2013, p. 9).

3. Methodology: Approach

3.1. Research Concept

According to Brace (2013, p. 6) the definition of the research objective represents the first step of an empirical analysis. The ultimate aim of this study is the development of an appropriate framework and providing a set of recommendations to ensure the proper operational handling of cryptocurrencies. Therefore, the study identifies the following three research questions (cf. Chapter 1.1):

- What are the potential risks and resulting threats of accepting cryptocurrencies as a payment method?
- Are the companies and the responsible employees aware of these risks, and how do they evaluate and address them?
- Are there any general control activities and recommendations necessary to ensure an appropriate risk management in the handling of cryptocurrencies?

In order to answer these questions, a research concept was developed based on a combination of literature and empirical analysis. Based on the literature review on cryptocurrencies (cf. 2.1) and ERM (cf. 2.2), the author derived and identified the potential risks of Bitcoin payments and divided them into operational, reporting, and compliance risks in Chapter 4.1. The risk identification approach follows the COSO IC Framework (cf. 2.2.2.2), wherein the subsequent empirical analysis focuses on the stage of the risk assessment and the corresponding control activities of the COSO IC Framework. The results obtained of the risk identification provide, on the one hand, the answer to the first research question and, on the other hand, the basis for the empirical analysis that follows.

In the second part of the research concept, the empirical analysis (cf. 4.2) is conducted starting with an analysis of the general payment process. This is important to understand if there is any third-party intermediary (i.e., a payment processor) involved that already covers any risks and, moreover, to comprehend how the company deals with the incoming funds. Afterwards, the explicit administration of Bitcoin payments in a company will be addressed, which focuses on private key storage and its corresponding responsibilities. Further, the survey participants were tasked with conducting an assessment of the potential risks that were previously identified with regard to Bitcoin payments. Their responses will help answer the research question of to what extent companies are aware of and how they evaluate risk potential and severity. Finally, the current risk measures – provided that there are internal controls implemented – will be analyzed.

In the third and last step, the paper outlines specific recommendations in the form of a risk control matrix, which is based on a summary of the previous results (cf. 4.3.1). Furthermore, the author presents a more general and holistic approach, called the "Cryptocurrency IC Framework" (cf. 4.3.2) that was established following the COSO IC Framework. The framework integrates the results of this thesis. By combining the Cryptocurrency IC Framework and the developed risk control matrix, this thesis presents the recommendations necessary in order to ensure the appropriate operational management of cryptocurrencies.

3.2. Research Method

A research method can be defined as a "system for collecting information" that should be based on an "architecture that serves a theme or multiple themes" in order to yield a well-constructed data (Azzara, 2010, p. 16; Sue and Ritter, 2007, pp. 1-2). For the empirical analysis of this thesis, the author decided to employ an online survey with integrated display logics and redirection functions (see "survey" in Appendix 5). The survey required the participants to answer a series of questions within a certain time frame, which is necessary to ensure a considerable response rate and enhance the representativeness of the sample (Azzara, 2010, p. 25).

There are, of course, many different ways to conduct a survey, e.g., face-to-face interview, phone interview, written

interview, or online interview (Blasius and Baur, 2014, p. 662). An online questionnaire is an appropriate research tool in case of a fairly large sample that is geographically distributed (Blasius and Baur, 2014, p. 662). Moreover, Sue and Ritter (2007, pp. 13-14) state that the online option is well suited to sensitive questions because of its anonymity, and it prevents any bias in the responses through the absence of an interviewer (Brace, 2013, pp. 23, 26).

The ultimate goal of a questionnaire "is to meet research objectives by obtaining valid data from respondents who are properly screened and qualified" (Azzara, 2010, pp. 18-19). Therefore, a representative sample for the entire population has to be identified (see Chapter 3.4). In addition to the selection of a representative sample, the objectivity, reliability, and validity concerning the research data plays a significant role (Blasius and Baur, 2014, p. 72).

As described in the previous paragraph, objectivity can be ensured by a large sample and an appropriate research method, such as an online survey, in this case. Research validity and reliability can be improved by applying the concept of triangulation (Flick, 2011, p. 16), which refers to "the combination of methodologies in the study of the same phenomena" (cit. in Flick, 2011, p. 13). Therefore, the questionnaire for this thesis was designed to include qualitative and quantitative questions, which are intended to supplement each other (Blasius and Baur, 2014, p. 42). Whereas the qualitative questions are used to describe, interpret, and comprehend interdependencies, the quantitative questions provide numbers and values aimed at quantifying complex issues in an objective manner (Buber and Holzmüller, 2009, p. 73).

3.3. Research Measurement

The author Ian Brace (2013) states that responses to quantitative questions are generally measured using four kinds of data types and associated scales:

- Nominal data, which can be classified "into discrete categories by name" (p. 48)
- Ordinal data, which represents ranking scales without measuring the interval between each rank (p. 49)
- Interval data, which "provide[s] a rating for each item on a scale that has a numerically equal distance between each point" (p. 51)
- Ratio data, which is a special type of interval scale because the zero point has real meaning (p. 53)

This study employs nominal scales, ordinal scales (e.g., in the form of a Likert scale ranging from 1 to 5), and interval scales (e.g., a 10-point rating scale).

However, qualitative questions are assessed and evaluated through the concept of inductive content analysis. Inductive content analysis is recommended when the level of knowledge about a phenomenon is rather low or limited. Therefore, an inductive approach is more appropriate for studies intended to derive a theory from raw data rather than to verify an existing theory (Elo and Kyngäs, 2008, p. 107). The process of analysis of this method consists of three main stages: preparation, organization, and reporting (cf. Figure 13). However, the main function of content analysis is to classify as many words as possible from a text and to summarize the results in a proper model, conceptual map, or categories (Elo and Kyngäs, 2008, p. 107).

3.4. Sample

Before a survey can be developed and distributed, a representative sample has to be defined (Brace, 2013, p. 7). For this empirical study, it was quite difficult to select a representative sample because there is no transparent information available on how many companies accept Bitcoin payments.

According to the merchant service provider Coinbase (2018, 12. February), globally, over 48,000 merchants use its payment processor service. In contrast, the Bitcoin acceptance map called "coinmap.org" displays 11,400 globally registered venues at the time of writing this thesis (Coinmap, 2017, 21. September). A more specific source is btc-echo.de, which gives information about 250 companies accepting Bitcoin in Germany, Switzerland, and Austria and, moreover, there are about 30 multinationals accepting Bitcoin payments (BTC Echo, 2017).

In consideration of the aim of the research questions and the general lack of research available on this topic, this empirical analysis had no specific limitations – the only requirement was that the company had to be registered in Europe. There were no limitations on any particular industry, geographical area, or source of Bitcoin-accepting companies mentioned in the previous paragraph. This implies that this thesis focuses on gathering as much information as possible that can be justified by the research aim of developing a general and holistic framework. Based on these assumptions, the author created a random sample in the form of an Excel spreadsheet including the addresses and corresponding contact person (if any).

The survey was sent to 346 companies/institutions registered in European countries, with the majority (77.72%) being registered in Switzerland, Germany, and Austria. The type of organization ranged from micro-businesses to large corporations. The online survey was initially developed in English and then translated into German. When applicable, the cover letter was personalized, else the survey was sent with a general cover note (cf. Appendix 4).

From November 22 to December 15, 2017, the online survey was fully completed by 65 companies, which is a response rate of approx. 18.79%. An overview of the participants' industries can be seen in Figure 14.

The majority of the survey participants belonged to the retail industry (32.31%), the tourism sector (13.85%), and IT (13.85%). Furthermore, a considerable number operated in the areas of legal, tax, finance, or controlling services (9.23%), other services (7.69%) and in the healthcare industry (6.15%). The remaining quarter was represented by other industries, with a more detailed listing shown in Figure 14.

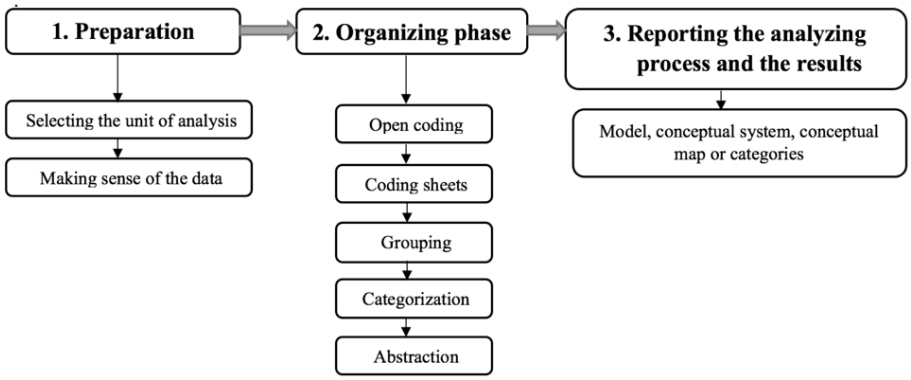


Figure 13: Inductive Content Analysis; Source: Own illustration according to Elo and Kyngäs (2008, p. 110)

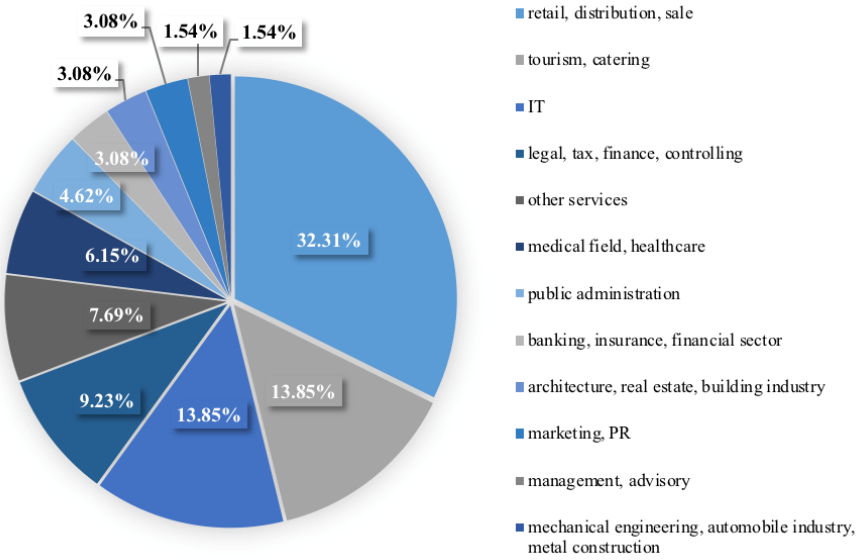


Figure 14: Industry-wide Distribution of Survey Participants

The participating organizations mainly ranged from micro- to small-businesses, with:

- 86.15% having up to 9 employees and up to € 2 million revenue/year (micro-business)
- 9.23% having up to 49 employees and up to € 10 million revenue/year (small-business)
- 3.08% having up to 249 employees and up to € 50 million revenue/year (SME)
- 1.54% having more than 249 employees and over € 50 million revenue/year (large corporation)

With regard to the share of Bitcoin payments (measured as the percentage of total amount of incoming payments), the vast majority (78.46%) indicated that less than 1% of incoming funds are currently paid in bitcoins. However, 18.46% of the participants stated that their share of Bitcoin payments is 1-5% while 3.08% stated the percentage is 5-20%.

4. Methodology: Results

4.1. Risk Identification of Bitcoin

According to Arwinge (2012, p. 45) and the COSO IC Framework (Section 2.2.2.2), risks can be classified into the following three categories:

- Operational risks related to the effective and efficient use of resources
- Reporting risks that might affect financial reporting quality
- Compliance risks representing any breaches of applicable laws and regulations

The identification of risks serves as the basis of empirical risk assessment and, thus, helps answer the research question related to how risks should be evaluated, managed, and controlled by an organization. Therefore, the author has identified and summarized the risks of Bitcoin that might negatively affect an entity's operational, reporting and compliance objectives in order to answer the first research question

and, moreover, to provide the basis for the empirical analysis in Chapter 4.2. Additionally, the potential implications (PI) and potential control activities (PCA) are outlined at the end of each sub-section in the form of a table.

- What are the potential risks and resulting threats of accepting cryptocurrencies as a payment method?

4.1.1. Operational Risks

A lack of know-how

Cryptocurrencies have emerged with the completely new invention of blockchain technology. Due to the properties of this technology and the way in which it is used to conduct transactions, there are considerable differences in how payments are dealt with compared with other payment methods.

In general, a lack of know-how aggravates all emerging vulnerabilities and risks associated, which will be presented in the following paragraphs. In particular, a lack of know-how with regard to the administration of cryptocurrencies, the purpose of the public and the corresponding private key, and the concept and properties of cryptocurrencies might have implications ranging from reduced operational efficiency to a total loss of all bitcoins that a company owned (provided the company uses only the hot storage option limited to one wallet). In this context, it has to be emphasized that an executed transaction is irreversible, so there is no possibility to recover these lost bitcoins.

A solid education and training on cryptocurrencies might aid the effective prevention and mitigation of these vulnerabilities as well as the associated risks. It is not a prerequisite for a company and its employees to completely understand blockchain technology in order to implement the acceptance of Bitcoin payments. However, a basic understanding of the technology and the necessary risk awareness/evaluation is required. To sum up, a lack of knowledge could have a vast (negative) impact on a company's effective and efficient resource use.

> PI: Total loss of all bitcoins, misuse of superior knowledge to commit (irreversible) fraud due to internal or external circumstances, operational losses/ inefficiencies
> PCA: Employee training, periodical updates on crypto-markets and price developments, manuals

The Administration of Cryptocurrencies

As previously described, bitcoins are digital files "with a cash value in the hands of the individual in possession of the file" (Grant and Hogan, 2015, p. 32). If this digital value were to be stolen, the company would have no further opportunities to access its initial bitcoins, and they would finally be lost as there is no way to easily trace back the transaction and reverse it. This is comparable to losing one's purse and all the cash inside it (Choo, 2015, p. 300). Particularly with regard to the dealing and storage of this digital value, an organization's management must address two interrelated questions: first, who is responsible for the (private) key administration and, second, how is this key to be stored?

The owner of the private key has the full access rights and ownership of the corresponding bitcoins, which implies that safekeeping is the most important role in the operational dealing of cryptocurrencies. In a risk report, the insurance company Lloyds (2015, p. 7) described the private key as a digitized "secret such as banking credentials, intellectual property, or private photographs," which could be or could become a decisive factor in an organization's success.

Therefore, it plays an important role in not only the administration of this key within a company but also in clearly determining the responsibilities and duties concerning the administration of the bitcoins received. In this context, there is also the possibility to outsource the private key's administration to an intermediary or an external provider like a payment processor or an exchange platform (Lloyds, 2015, p. 7). Key storage by an external provider offers the advantages of a professional and secure administration (Franco, 2014, p. 131; Grant and Hogan, 2015, p. 33). However, this is also related with additional costs and risks, especially with regard to the reliability of an external service provider. History has already unveiled such risks; for instance, the exchange platform Mt. Gox was hacked in 2011 and 2014 which resulted in around 650,000 bitcoins being stolen from its customers and the company finally suffering insolvency (Hern, 2014, 18. March).

Regardless of whether storage is outsourced or not, there are in general two types of wallets used to keep bitcoins: hot and cold storage wallets. Blockchain researcher Toshendra Sharma (2017, 14 November) states that a hot wallet can be compared with a checking account, whereas a cold wallet is a kind of savings account. The question then arises of which type of wallet a company chooses and how these wallets will be secured. Although a cold wallet is an offline wallet that is not connected to the Internet, hot wallets or web wallets are stored on devices that are connected to the Internet and directly communicate with the Bitcoin network (Franco, 2014, p. 126).

This cold storage option is available in several forms: the private key could be saved on an external media storage (e.g., USB flash drives or optical disks), on a paper wallet (by printing the private key on a piece of paper), or on a special hardware wallet like Trezor (Antonopoulos, 2015, p. 237; Franco, 2014, pp. 126f.). The benefit of a cold wallet is that it is secure against hacker attacks, but due to their physical and tangible form, they require appropriate storage facilities like a vault (Franco, 2014, pp. 17-18). In contrast, a web-based wallet is usually provided by an external provider and is in the form of an online account (with additional features) in which funds can be deposited and accessed, similar to online banking (Franco, 2014, p. 131). Users can access the account by means of an authentication process (e.g., 2-factor authentication or multi-signature), after which they can conduct transactions. Additionally, the use of a hot wallet is more appropriate in order to accept payments because of a faster verification process (Sharma, 2017, 14 November).

Depending on the choice of wallet type and/or third-party involvement, the safekeeping of keys requires appropriate cyber security measures, physical protection, or both. In general, it is recommended to store larger amounts of cryptocurrency assets in cold wallets, while hot wallets would be a better choice for daily operations. (Antonopoulos, 2015, p. 237; Sharma, 2017, 14 November)

> PI: Total loss of bitcoins due to inappropriate hot storage, physical theft due to unreasonable cold storage, employee fraud in operational dealings
> PCA: Outsourcing of "cold" private key storage, e.g., in the vaults of multinational banks, limitations of access rights to the company's wallet, multi-signature wallets, encryption of private keys, diversification of bitcoins (hot and cold wallets), implementing holding limits on the hot wallets

IT Risks

Particularly in the context of IT, recent technological innovations have led to the emergence of new risks. The two kinds of risks associated with Bitcoin are global and local. Global risks or "attacks" are aimed at manipulating the entire Bitcoin network, while local risks or "attacks" are characterized by the intention to get specific access to a private key or password of a company's hot wallet "in order to gain control of bitcoins and the matched public address" (Lloyds, 2015, p. 7). On account of significant price developments and the resulting increase in the value of bitcoins, the cryptocurrency is an extremely attractive target for hackers and thus for local attacks. This is further encouraged by the instant diversion and irrevocability of transactions without the need of converting "identity information or account tokens – such as credit cards, and bank accounts – into value after compromising them" (Antonopoulos, 2015, p. 236).

Therefore, vendors accepting Bitcoin should be aware of the importance of private keys (or wallet passwords). For instance, they should not store this key in the form of any other data file (including encrypted files) on their desktop computers (Antonopoulos, 2015, p. 236). However, the risk of a local attack can be mitigated by means of appropriate cyber security measures, the necessary know-how, and the appropriate distribution of coins on different storage mediums.

Controversially, global risks (e.g., a 51%-attack or a Distributed-Denial-of-Service (DDoS)-attack) which are closely related to some vulnerabilities of blockchain technology, cannot usually be controlled and influenced by the company itself (Lloyds, 2015, pp. 10f.). The scope of this thesis, however, does not cover an in-depth analysis of these IT-related (blockchain) risks.

> PI: Private key/ password theft (depending on whether hot or cold storage) through hacking, skimming, etc., and the resulting operational losses
> PCA: Appropriate IT infrastructure/ risk management, implementation of additional encryption standards, several storage options (hot and cold storage)

The Irreversibility of Transactions

In general, the irreversibility of transactions can be seen as an advantage but also as a source of some risks. For instance, if a local attack were to be successful and the "thief" were to gain access to a company's private key, the bitcoins could be grasped immediately and distributed to different wallet addresses (Lloyds, 2015, p. 8). In such a case, there would be no possibility of reversing the transactions, i.e., there is no charge-back option such as in the case of a disputed service by a credit card provider (IMF, 2016, p. 29; Vigna and Casey, 2016, p. 127). Moreover, one has to keep in mind that a customer has no right to refund a transaction. If anything goes wrong, the risks of default payments have to be covered by the Bitcoin network participant or the Bitcoin accepting vendor, because there is no central authority that has the responsibility to do so (IMF, 2017, p. 29). This makes a fraud case especially challenging since there is no relevant authority that could freeze or seize an order (IMF, 2017, p. 28).

However, this irreversibility can also be an advantage given the new digital business models, e.g., when digital files are instantly delivered and cannot be reversed, like in the case of the download of songs or software (Sixt, 2017, p. 89).

> PI: Operational losses due to default payments, wrong transactions, and fraud
> PCA: n/a

4.1.2. Reporting Risks

Reporting Standards

Grant and Hogan (2015, pp. 30-31)argue that the explicit reporting and classification of the bitcoins received depends on their usage, i.e., either as a medium of exchange or as an investment. Nevertheless, there is not yet a consistent regulation concerning the explicit classification of bitcoins (Lindner and Meyer, 2017, p. 29). In the following paragraphs, the reporting of bitcoins will be analyzed in the context of Germany and Switzerland.

Lindner and Meyer (2017, p. 29) have questioned the explicit reporting of bitcoins as "liquid funds" in Switzerland, given their significant price volatility; however, it might be also possible if this requirement were to be fulfilled. According to Heer, 2014, 10. December, the classification of bitcoins as liquid funds is excluded. Instead, bitcoins should be reported as "short-term assets with market price" and thus should be classified as short- or long-term securities (Heer, 2014, 10. December; Lindner and Meyer, 2017, p. 29). In summary, the explicit classification depends on the usage of bitcoins, for instance, if the bitcoins are used for investment purposes and will be held for a longer term, the coins should

be classified as long-term financial assets such as commodities like gold or oil (Lindner and Meyer, 2017, p. 29).

In Germany, the analysis of Kanton (2017, p. 2735) reveals that according to the German Handelsgesetzbuch, bitcoins have to be reported as "other assets," part of the current assets, or as "acquired intangible assets" as part of the fixed assets. It is extremely important to comply with the national reporting standards, because a violation could lead to the fraudulent misrepresentation of the financial statements, an inaccurate company valuation, and issues with tax evasion.

> PI: (Fraudulent) misrepresentation of financial statements, inaccurate company valuation, evasion of tax
> PCA: Establishing guidelines for the national reporting of Bitcoin

The Price Volatility & Exchange Rate Risks

One of the most common risks with cryptocurrencies and, Bitcoin especially, is the considerable degree of price volatility. Appendix 2 contains an extracted chart of the Bitcoin/USD spot rate from January 16, 2017, to January 16, 2018. It shows the significant volatility of the cryptocurrency. Whereas one bitcoin was traded at around USD 800 at the beginning of 2017, the value increased by 1400% to approx. USD 12,000 in January 2018. In order to further exhibit these price fluctuations, the Bloomberg "Return-on-Change" function (the yellow line below the price index chart) was added. This function is a technical indicator of volatility, measuring the price change between current price and the price ten days ago in percent. Therein, substantial fluctuations of 20% are no rarity.

The extreme price volatility of incoming funds first has an impact on the exchange rate risk (FX risk), i.e., the price at which the bitcoins will be converted into national currencies. In turn, this might affect the entity's effective and efficient operational use of resources as well as the company's financial reporting.

With regard to operational effectiveness, it can be primarily stated that the received funds could appreciate but also depreciate within in ten days by about 15-20% (cf. Appendix 2), and thus significantly affect the operational revenue within a very short period of time. In addition, assuming that the company uses Bitcoin funds for operational purposes and as a medium of exchange, it could even lead to liquidity shortages or considerable FX losses, for instance, in case of paying a supplier if the price drops by about 20% in 72 hours (Grant and Hogan, 2015, p. 30).

Financial reporting might also be influenced by these FX fluctuations. On the one hand, it is quite difficult to match any revenue forecasts or conduct appropriate budgeting (Hoelscher, 2014, p. 24). On the other hand, depending on the usage of Bitcoin and the applicable national law, the exchange of bitcoins in national currencies could result in tax charges.

> PI: Operational losses due to FX fluctuations, liquidity shortages, tax charges, inability to convert Bitcoin into other currencies due to a lack of liquidity
> PCA: Hedging of bitcoins, instant conversion by means of a payment processor, establishing guidelines related to the monitoring of liquidity in Bitcoin markets

4.1.3. Compliance Risks

Tax-Compliance

In general, more is known about the taxation of Bitcoin than about its financial reporting (Lindner and Meyer, 2017, p. 28). Nevertheless, cryptocurrencies exhibit a high potential for tax evasion due to the fact that participants do not need to disclose their identity, and there is no means to identify beneficial owners (IMF, 2016, p. 30). For appropriate tax treatment, it is first important to know who is the subject of the tax, i.e., a natural person or a judicial body. Additionally, there is also the question of the classification of bitcoins, i.e., whether it is a form of currency or a short- or long-term security.

In case of a judicial body, the received payments have to be recognized in the income statement (calculated in the national currency by the time the funds are received) and could be further activated in the financial statements (see Section 4.1.2). If they are instantly converted to fiat currencies, they will be recognized as revenue, and there would be no further tax issues. Controversially, if the bitcoins are held as short- or long-term security, the resulting capital gains (in case of realization) would be additionally subject to the corporate income tax in Switzerland or the personal income tax and corporate income tax in Germany (Lindner and Meyer, 2017, p. 29; Schmidt, 2018, 18. January).

In Switzerland, a natural person is not faced with any specific tax-compliance issues if the bitcoins are used for private purposes, and even if any capital gains are realized with exception of Swiss property tax (Kanton, 2017).

In contrast, in Germany, any bitcoin capital gains are subject to German income tax regulations. Only if a natural person holds the bitcoins for a period longer than one year, are the achieved capital gains tax free (Schmidt, 2018, 18. January). The relevant valuation method is the first-in-first-out method, which can be made transparent by means of the blockchain (Schmidt, 2018, 18. January).

> PI: Tax evasion and its legal implications
> PCA: Establish guidelines for the recognition and valuation of Bitcoin transactions with an emphasis on regulatory compliance

Anti-Money-Laundering and Know-Your-Customer Issues

From a financial integrity perspective, the properties of Bitcoin do raise concerns, particularly with regard to its anonymity and the cross-border reach of transactions (IMF, 2016, p. 27). Although every transaction is publicly available, the users are virtually anonymous (Grant and Hogan,

2015, p. 32). This implies that the concept of Bitcoin has a high degree of transparency in the transactions conducted but not with regard to who has conducted the transaction. This is sometimes described as pseudo-anonymous, because of which cryptocurrencies are fundamentally vulnerable to money laundering. The IMF (2017, p. 27) states that bitcoins can be used "to conceal or disguise the illicit origin or sanctioned destination of funds, thus facilitating money laundering (ML), terrorist financing (TF), and the evasion of sanctions." Furthermore, bitcoins are likely to be used for cyber-related crimes, e.g., on the "dark web" or as ransom money to decrypt data previously encrypted by malware.

Regulators have adopted different approaches to mitigate these risks (cf. Chapter 2.1.4). In general, only financial intermediaries are faced with AML- and KYC-related regulations, so the vendors and their users have not yet faced these compliance issues (IMF, 2016, p. 28; Piller, 2017, pp. 8-9; Choo, 2015, p. 304). This implies that a vendor accepting Bitcoin has to take appropriate measures to ensure that his customers are in line with the KYC- and AML- related laws.

> PI: Accepting illicit funds, being liable to prosecution
> PCA: Customer due diligence, reporting of suspicious transactions

4.2. Empirical Analysis

The following empirical analysis confronts the participating organizations with the risks identified in order to answer the second research question:

- Are the companies and the responsible employees aware of these risks, and how do they evaluate and address them?

4.2.1. Payment Process

If a company accepts Bitcoin payments, it is first necessary to understand how it receives and deals with them, i.e., to what extent the transaction process is self-managed and for which purposes the received bitcoins are used.

The analysis reveals that 44.62% of the participants employ a merchant service provider to process the incoming Bitcoin funds, whereas 55.38% indicated that they manage the payments without any third-party involvement (cf. Figure 15). Since the use of a payment processor can help mitigate or eliminate some emerging risk factors (e.g., the FX risk or the payment default risk), the analysis made a distinction between participants who do and do not use merchant service providers.

We found that around half of the participants in our survey use payment processors. Although there are many reasons behind this decision, Figure 16 enable the derivation of two overriding reasons.

Note: The participants were allowed to choose multiple answers and the sum of the results is therefore over 100%.

Figure 16: Reasons for Using a Payment Processor The first reason is the mitigation of risks. Among the respondents, 62.07% mentioned using payment processors for the prevention of the FX risk through the possibility of instantly exchanging bitcoins into fiat currencies, and 44.83% cited covering a potential payment default due to the immediate payment confirmation and the liability of the merchant service provider. Moreover, the appropriate documentation and invoicing that is closely related to appropriate financial reporting and the resulting reporting risks, was mentioned by 31.03% of the participants.

The second dominant reason for involving a merchant service provider was for simplification and convenience, which leads to lower entry barriers for potential vendors accepting Bitcoin payments. In fact, 58.62% of the respondents justified using a merchant service provider because of the infrastructure provided, such as a shopping cart plugin-in for e-commerce or applications and interfaces for point-of-sales. Furthermore, even 58.62% of the participants cited implementing a payment processor because it enables the acceptance of Bitcoin payments without in-depth knowledge.

The analysis also investigated the other half of participants who do not use third-party providers because of its potential redundancy and the costs involved. Therefore, the analysis focused on the awareness of risks that might be potentially covered or mitigated by means of payment processor, i.e., the FX risk, defaulting payments and the proper documenting and invoicing which is closely related to reporting and tax risks.

The results show that 80% neither experienced a payment default nor viewed the documentation and invoicing as a pitfall, which is consistent with the initial assumption that a payment processor would be redundant. Controversially, the FX risk which could be almost completely eliminated, was mentioned by 45.71% of the participants as a risk, and 37.14% recognized the reporting and tax issues as a risk.

This study also addressed the question of how a company deals the incoming Bitcoin funds. In general, there are two different possibilities: either bitcoins are only used as a payment method and they will be instantly exchanged into national currencies, or the bitcoins will be held by the company for use as liquid funds or as an investment. In this context, storage plays a critical role, because if the bitcoins are used as an investment or as a liquid fund in order to pay invoices or suppliers, the company needs an appropriate Bitcoin administration. Controversially, if the bitcoins are exchanged immediately or on the following day, the Bitcoin storage becomes more or less obsolete.

The pie chart in Figure 17 shows the results concerning the handling of incoming Bitcoin payments. It is apparent that almost 62% (using cryptocurrency as liquid funds or investment) of the respondents store the incoming funds, whereas around 38% exchange incoming funds instantly or by the following day.

The 62% of participants storing the funds are especially faced with the threat of proper Bitcoin administration and all its related risks. Hence, the second part of the empirical investigation analyzes the administration and duties related to Bitcoin payments.

In summary, the first part of this evaluation concerning

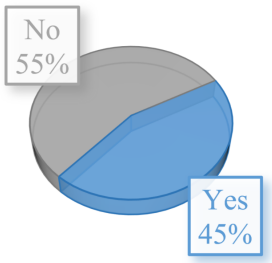


Figure 15: Third-Party Involvement in the Payment Process

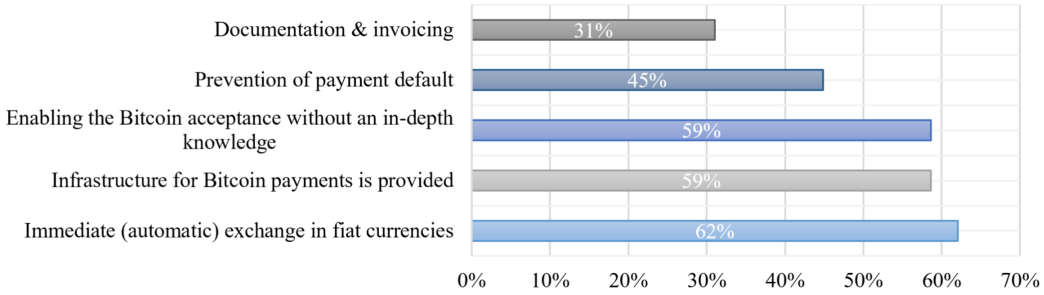


Figure 16: Reasons for Using a Payment Processor; Note: The participants were allowed to choose multiple answers and the sum of the results is therefore over 100%.

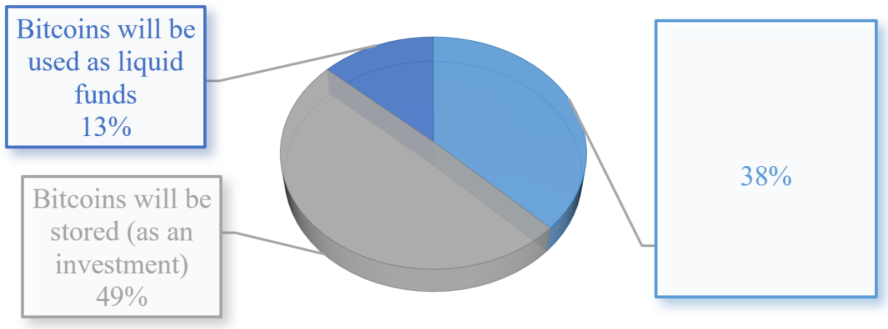


Figure 17: Dealing with Incoming Bitcoin Funds

the payments process reveals that there is no definite trend of how this process plays out in practice, i.e., with or without a merchant service provider. This implies a considerable issue for the development of a proper Cryptocurrency IC Framework, because all potential risks have to be addressed. Furthermore, the results of the present study demonstrate that the use of a payment process is justified by two reasons: risk mitigation/elimination and the purposes of simplification and convenience. In context of risk mitigation, the FX risk was mentioned as the greatest danger which could be basically eliminated. Moreover, approx. two thirds of the companies store the incoming funds and are thus confronted with a reasonable administrations of Bitcoin payments.

4.2.2. Administration of Bitcoin Payments

It is important to understand that there is not necessarily a connection between Bitcoin storage and the involvement of a payment processor. Even though a kind of third-party provider is employed, cryptocurrencies might be transferred and stored in one's "own" wallets. Therefore, the crucial question is if the bitcoins are stored or not, whether in the form of an investment or as liquid funds, as discussed in the previous chapter.

When bitcoins are stored, a company is faced with several options that are listed in Figure 18.

As can be seen in Figure 18, the analysis indicates that the majority of participants (40.54%) store their bitcoins in a merchant service provider's wallet. In this context, the private key storage is outsourced, with the resulting risk of third-party reliability. When only the hot storage method is used

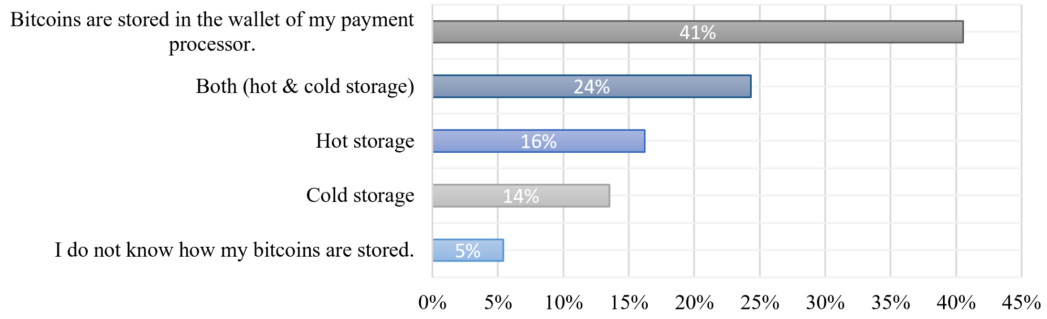


Figure 18: Options for Bitcoin Storage

(16.22%), the company faces the same advantages, but the difference is that the risk of third-party reliability is due to the wallet provider and not the payment processor. In both cases, the administration of rights to access the third-party wallet plays a significant role.

Moreover, we found that 24.32% of companies use both methods, and 13.51% only use the cold storage option. Therefore, the storage and administration have to be clearly determined. Finally, 5.41% of the respondents stated that they did not know how their bitcoins are stored.

In addition to Bitcoin storage, this study also investigated who is generally responsible for the administration of bitcoins, i.e., who has the right to access the private key or wallet and to which field of competency this duty is assigned. Several noteworthy results in this context were the answers "nobody" and "everybody" in response to the question, "Who has the admission or the relevant rights to access your company wallet?". With the exception of these answers, the majority of participants (90.91%) mentioned that a specific person has access to the company's wallet. The responsible persons are typically the Chief Executive Officer (CEO), Chief Digital Officer (CDO), IT Administrator or Head of Accounting, as well as their assistants or representatives.

Responses to the question regarding the number of people who have the access rights ranged from one to ten employees, with an average of two persons having the rights to access the wallet. With regard to their field of competency, this duty is typically assigned to the senior management (CEO, CDO, Chief Technology Officer (CTO) or the Chief Financial Officer (CFO)), or an executive manager such as the IT Administrator or the Head of Accounting.

4.2.3. Risk Awareness & Evaluation

The third part of the empirical analysis focused on the awareness and evaluation of the risks identified in Chapter 4.1.

The respondents were first asked to describe their awareness of the risks by evaluating if there is a risk potential in general and how likely it is that this risk will occur. It was possible to choose from five options ranging from "no risk" to "extremely high risk." The results are summarized in Figure 19 below.

The data suggests that the experienced potential of the risks identified is rather low. In particular, the irreversibility of the transactions does not pose a risk for 40.32% of the participants, whereas 27.42% rated it as a low risk, and 20.97% as a moderate risk. This implies that only around 5% considered the irreversibility of the transactions to be a threat. Furthermore, risks related to the financial reporting and taxes were rated comparatively low. In contrast, the price volatility and the resulting FX risk of Bitcoin exhibited the highest risk potential, with 23.44% of the participants classifying it as an extremely high risk and 18.75% as a high or moderate risk. Moreover, a lack of know-how, risks within the administration of Bitcoin, and cyber risks were ranked as moderate risk or greater by at least 45% of the participants.

Besides the risk evaluation, the results shown in Figure 19 also reveal that 9.52% of the participants were not able to assess the compliance risks. With regard to the blockchain risks (7.81%), the cyber risk (6.35%), the financial reporting risk (6.25%), and the irreversibility of transactions (6.45%), an increased uncertainty related to the evaluation of the risk potential was also apparent.

Nevertheless, in order to clearly interpret the results, the authors calculated the mean of the risks evaluated (no risk – 1, extremely high risk – 5) based on the responses. Subsequently, the risks were classified and ranked according to their classification and risk potential, which can be seen in Table 3.

The analysis also aimed at investigating the severity of the potential of damage that could be caused by the risks identified. Here, the participants had the option to evaluate the risk severity by choosing a number between one and ten in order to assess and further express the damage potential from their point of view. Here, one represented a low or almost no damage potential, and ten an extremely high damage potential. The results can be seen in Table 4.

The figures reveal that the companies generally assess the severity of potential damages as low. Their greatest concerns are about risks related to FX, cyber, and blockchain. Controversially, financial reporting, compliance, tax risks, and the irreversibility of transactions are considered to have a lower potential for damage.

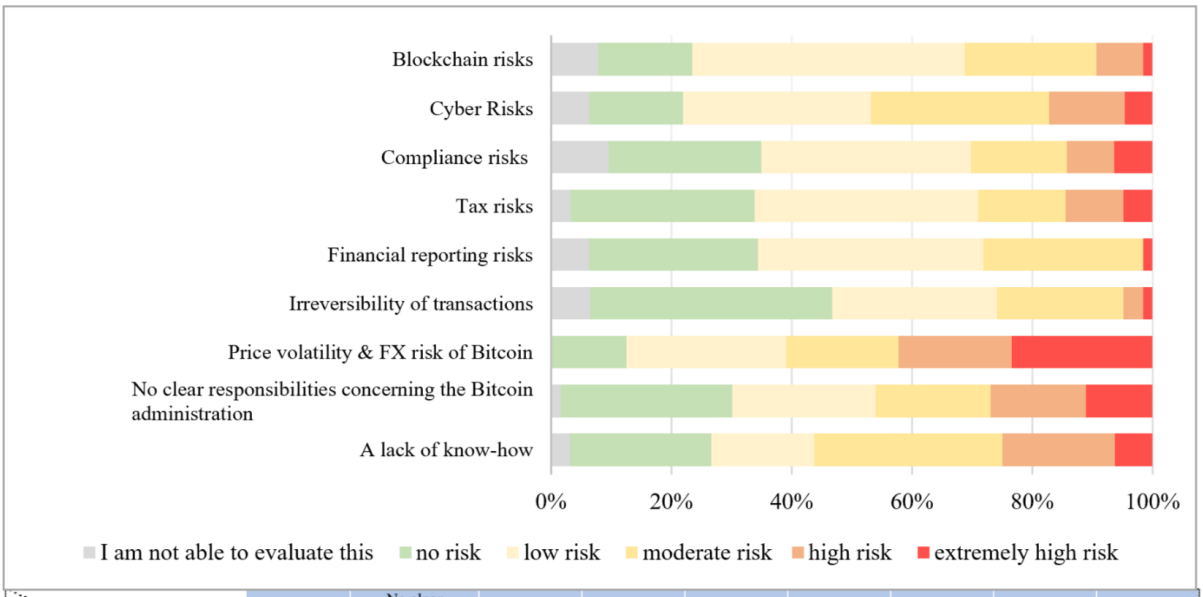
These results have been summarized in a risk matrix cre-

Table 3: Evaluation of the Risk Potential

	Price volatility & FX risk of Bitcoins	A lack of know-how	Cyber Risks	No clear responsibilities concerning the Bitcoin administration	Blockchain risks	Compliance risks	Tax risks	Financial reporting risks	Irreversibility of transactions
Mean	3,14	2,66	2,57	2,56	2,29	2,28	2,18	2,03	1,91
Risk Classification	moderate	low - moderate	low - moderate	low - moderate	low	low	low	low	low

Table 4: Evaluation of the Risk Severity

	Price volatility & FX risk of Bitcoins	Cyber Risks	Blockchain risks	A lack of know-how	No clear responsibilities concerning the Bitcoin administration	Financial reporting risks	Compliance risks	Tax risks	Irreversibility of transactions
Mean	3,66	3,58	3,37	3,08	3,04	2,96	2,95	2,7	2,02
Risk Severity (damage potential)	low - moderate	low - moderate	low - moderate	low - moderate	low - moderate	low	low	low	low



	A lack of know-how	No clear responsibilities concerning the Bitcoin administration	Price volatility & FX risk of Bitcoins	Irreversibility of transactions	Financial reporting risks	Tax risks	Compliance risks	Cyber Risks	Blockchain risks
I am not able to evaluate this	3.13%	1.59%	0.00%	6.45%	6.25%	3.23%	9.52%	6.35%	7.81%
no risk	23.44%	28.57%	12.50%	40.32%	28.13%	30.65%	25.40%	15.87%	15.63%
low risk	17.19%	23.81%	26.56%	27.42%	37.50%	37.10%	34.92%	31.75%	45.31%
moderate risk	31.25%	19.05%	18.75%	20.97%	26.56%	14.52%	15.87%	30.16%	21.88%
high risk	18.75%	15.87%	18.75%	3.23%	0.00%	9.68%	7.94%	12.70%	7.81%
extremely high risk	6.25%	11.11%	23.44%	1.61%	1.56%	4.84%	6.35%	4.76%	1.56%

Figure 19: Evaluation of the Risks Identified

ated by the author based on the data available. Taking into account the centered extract (cf. Figure 20) of the established risk matrix (the complete risk matrix can be found in Appendix 6), we can conclude that the FX risk is experienced as the greatest threat. Cyber and blockchain risks as well as the lack of responsibility concerning know-how and Bitcoin administration play a comparatively significant role. In particular, the irreversibility of the transactions was ranked as a lower risk.

4.2.4. Risk Handling

The last part of the empirical study deals with the potential and practical handling of the risks identified. We considered only those risks that can be effectively influenced by a company, for instance, a company cannot influence price volatility or blockchain risks but it can control the exchange rate or cyber risks.

The potential development of internal controls was analyzed in this regard. According to the results, especially regarding insufficient know-how and the segregation of duties (no clear responsibilities concerning Bitcoin administration), the development of internal controls seems possible. Around 70% of the respondents stated that the development is rather or absolutely possible. However, only 30% were of the opinion that it is rather not possible respectively impossible to develop internal controls in order to hedge the FX risk of Bitcoin. A detailed overview of these responses can be seen Figure 21.

In addition to the potential development, the practical implementation was also analyzed. In this context, only 46.15% of the companies have implemented internal controls or similar measures in order to ensure the appropriate dealing of Bitcoin payments (cf. Figure 22).

In this context, the explicit dealing was scrutinized, i.e., which specific internal controls or measures have been implemented. The results are summarized in Appendix 7 and serve as an important component of the risk control matrix provided in Chapter 4.3.1.

The results indicate that the risks identified are properly addressed only by a few companies. In order to overcome a lack of know-how, several organizations have implemented regular training sessions or workshops on cryptocurrencies, their purpose, and dealing. Some companies also provide their employees with manuals and have created internal guidelines intended to impart the knowledge required for operational business. The staff also gets the thus so far voluntary opportunity to watch YouTube tutorials during work hours as a form of e-learning, so as to increase their level of knowledge.

With regard to the appropriate administration and storage of bitcoins, many enterprises have decided to limit the responsibilities to an extremely small group of people, for in-

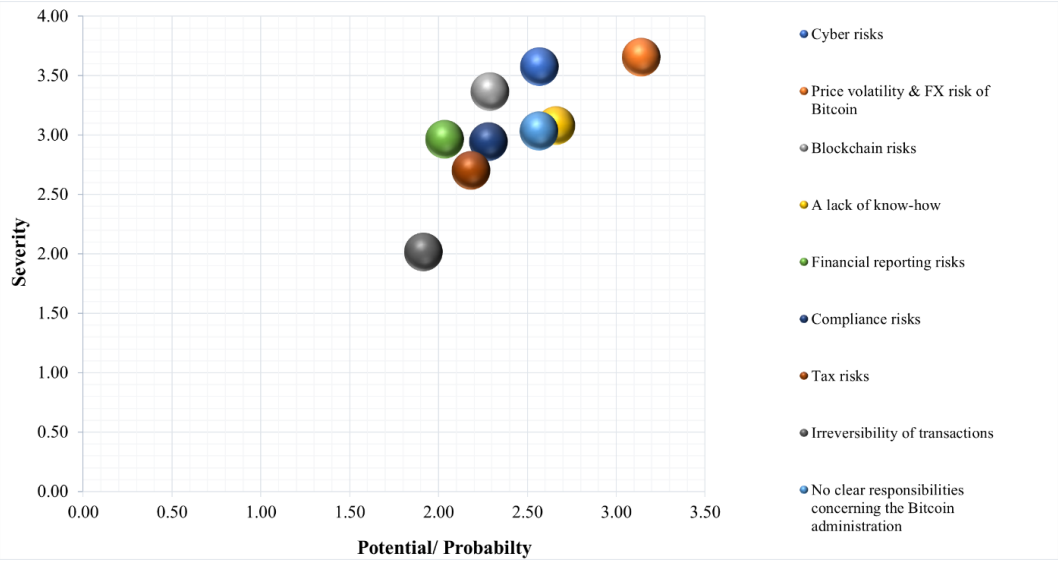


Figure 20: Extract of the Risk Matrix

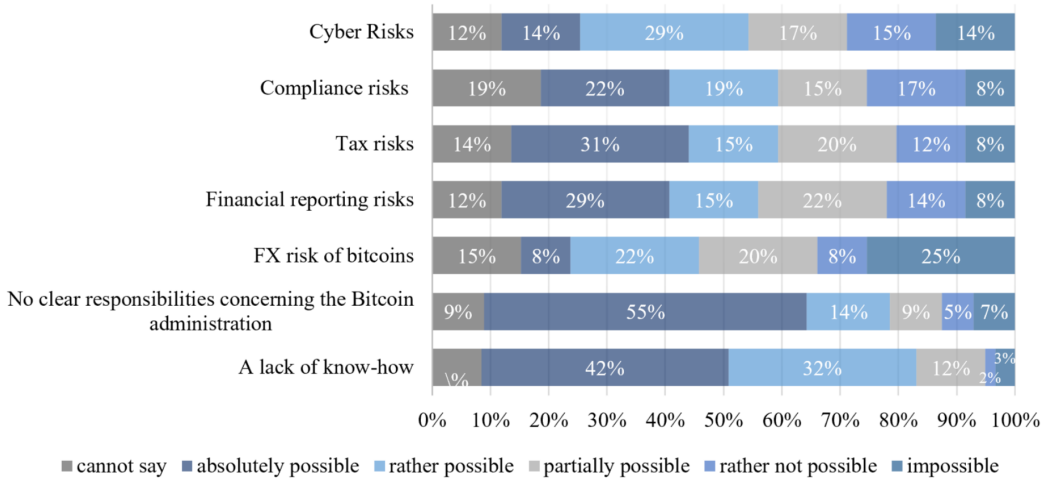


Figure 21: Development of Potential Internal Controls

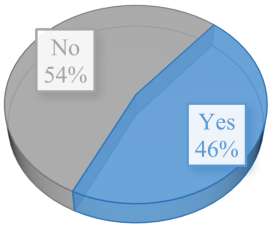


Figure 22: Implementation of Internal Controls

stance, only the CEO and his or her representative typically have rights to access the company's wallet. In this context, several companies emphasized that the responsibilities have to be clearly documented and executed in order to prevent a segregation of duties. The storage options have already been explicitly analyzed in the previous chapters; however, a few companies were of the opinion that the cold storage itself represents a form of control measure. Additionally, one company is using a software that encrypts the corresponding pins/keys to further enhance its level of security.

The FX risks and the relevant internal controls are more or less obsolete if an enterprise instantly converts its received

Bitcoin funds into fiat currencies. As previously discussed, most companies indicated that it is impossible or rather not possible to develop internal controls, which is consistent with the findings concerning the internal controls related to FX risks. Besides the opportunity to completely eliminate the exchange rate risk through instant conversion, the participants mentioned that observation, analysis, and relevant documentation are also internal control measures taken to mitigate the FX risk.

In the area of reporting risks – the identified financial reporting risks but risks related to tax-compliance – the implemented IC measures are quite similar. In both cases, the appropriate documentation and the "four-eyes" principle were mentioned as the most important internal controls. Nevertheless, manual control or the additional involvement of an external advisor was proposed as a useful supplementary measure.

Furthermore, the analysis revealed several interesting IC measures regarding risks related to KYC and AML issues. Primarily, it can be stated that some companies use additional KYC checks in form of an obligatory part of the payment respectively ordering process, with suspicious customers being immediately reported to the authorities. The internal mapping of public addresses to real customers/identities in order to get a more transparent customer profile is yet another approach. The involvement of an internal IT Forensic division was mentioned as an internal control as well. Apart from these measures, the permanent monitoring of changes in the national regulations is certainly required to overcome any compliance risks.

The involvement of an internal IT Forensic division (if any) plays a significant role in mitigating cyber risks as well. By means of such a division or through internal IT risk management, potential threats can be prevented or detected in their early stages. Conducting training sessions or workshops to enhance the risk awareness and knowledge of companies' employees is also an appropriate measure. If a company would like to bring down the cyber risks (of Bitcoin storage) to an acceptable level of risk, they could even consider using cold wallets and an additional encryption software.

4.3. Recommendations with Regard to Cryptocurrencies

Based on the results of the previous two research questions, the author established a risk control matrix in order to provide a clear overview and summary of the findings. These conclusions will be incorporated into a holistic Cryptocurrency IC Framework, which will be developed along the lines of the COSO 2013 IC Framework. This will finally lead us to the answer of the third research question:

- Are there any general control activities and recommendations necessary to ensure an appropriate risk management in the handling of cryptocurrencies?

4.3.1. Risk Control Matrix

The author has summarized the findings of the previous two research questions in the form of a risk control matrix to provide comprehensive and transparent overview of the risks identified and to outline recommendations concerning their handling. As proposed in Chapter 2.2.2.2, the matrix is divided into three superordinate categories – objectives, risk analysis and control activities – which will be further specified.

The first category of "objectives" is sub-divided in two sections: the first column shows the general objectives of the risk control matrix with regard to cryptocurrencies, and the second column categorizes the general objectives according to the three classifications proposed by the COSO 2013 IC Framework.

The following three columns represent a subdivision of the category of "risk analysis" and display the findings of the investigation. Therefore, it displays the identified risks (Chapter 4.1) and their corresponding risk potential and severity (cf. Chapter 4.2.3) as evaluated by the survey participants.

Finally, the last category summarizes the "control activities." This was done by selecting the appropriate measures proposed in the empirical analysis in Chapter 4.2.4 and by adding the potential control activities mentioned in Chapter 4.1. Additionally, the author assessed the types of controls (preventive = pr, directive = di, detective = de or corrective = cr) and the forms of the control activities, i.e., automated (a) or manual (m). The entire risk matrix can be found in Table 5.

4.3.2. Cryptocurrency IC Framework

The third research question also aimed at identifying general recommendations to ensure appropriate risk management in the handling of cryptocurrencies. Hence, the author decided to establish a framework that serves as a set of guidelines to implement and handle cryptocurrencies as a payment method and to ensure appropriate risk management.

The Cryptocurrency IC Framework developed is along the lines of the COSO 2013 IC Framework and adapted to cryptocurrencies based on the research results obtained through the example of Bitcoin. The framework can be seen Figure 23, with a higher resolution version in Appendix 8. Figure 23 shows a framework based on five processing steps. However, the established Cryptocurrency IC Framework does not present a "5-stages-model" – it should be rather understood as a continuous circle of processes. Moreover, it is important to understand that the framework represents a holistic approach and should thus be viewed as a whole and not just as a collection of its five components, each of which is described in further detail below:

1. Understand: Even though the analysis revealed that some or the other risk is experienced as more or less dangerous, the holistic model does not start by tackling specific risk factors. The fundamental prerequisite for the proper implementation and dealing of cryptocurrencies is a basic knowledge of its technology – the blockchain – the concept of a cryptocurrencies, the payment process, and the corresponding administration of

Table 5: Evaluation of the Risk Severity

Objectives		Risk Analysis			Control Activities		
General Objective	Classification of Objectives	Identified Risk	Risk Potential/ Probability	Risk Severity	Internal Controls/ Measures	Type	Form
following the COSO IC Framework		(cf. Chapter 4.1)	(cf. Chapter 4.2.3)	(cf. Chapter 4.2.3)	(cf. Chapter 4.2.4) + own supplementation	(own assessment)	
Development and maintainment of an internal control system with regards to cryptocurrencies that enhance the likelihood of achieving the entity's objectives relating to operations, reporting and compliance	Operational Objectives	A lack of know-how in dealing with cryptocurrencies	2.66	3.08	- establishing manuals and internal guidelines	pr/di	m
					- giving regular employee trainings/workshops	pr/di	m
					- providing regular market updates	pr/di	a/m
					- establishing a proper e-learning concept, e.g., YouTube tutorials & quizzes	pr/di	a/m
					- using multi-signature wallets	pr/di	a
					- outsourcing of private key storage/hardware wallets	pr/di	a/m
		A lack of clear responsibilities in relation with the Bitcoin administration	2.56	3.04	- limiting of responsibilites to a small group of persons	pr/di	m
					- access rights have to be clearly documented	pr/di	m
					- reading of the manual is required	pr/di	m
					- additional pin encryption, for instance by using the software keepass	pr	oca
					- using multi-signature wallets	pr/di	a
					- diversification of bitcoins to several wallets (hot & cold wallets)	pr/di	a/m
					- establishing limits of the bitcoin holding amount on hot wallets and transfer the excess number of bitcoins to cold wallets	pr/di	a/m
		Cyber risks	2.57	3.58	- implementing a reasonable IT risk management	pr/de/cr	a/m
					- establishing an internal IT forensic division	pr/de/cr	a/m
					- using cold wallets or outsourcing of private key storage	pr/di	a/m
					- giving regular employee trainings/workshops	pr/di	m
					- implementing additional pin encryption, e.g., by using the software "KeePass"	pr	a
	Reporting Objectives	FX risk of Bitcoin	3.14	3.66	- converting incoming Bitcoin funds instantly into fiat currencies	pr/di	a/m
					- hedging of Bitcoin positions through certificates (in case of an investment)	pr/di	a/m
					- appropriate documentation (amouts, FX rate, date and transaction details)	pr/di	a/m
					- obeseravation & documentation of FX rate	pr/di	m
		Financial reporting risks	2.03	2.96	- hiring a professional (external) advisor	pr/di	m
					- appropriate documentation (amounts, FX rate, date and transaction details)	pr/di/de	a/m
					- establishing guidelines for the national report of Bitcoin	pr/di	m
					- establishing guidelines related to the monitoring of liquidity in Bitcoin markets	pr/di	m
					- converting incoming Bitcoin funds instantly into fiat currencies	pr/di	a/m
					- manual review of transactions/ financial reporting	pr/de/cr	m
	Compliance Objectives	Tax risks	2.18	2.70	- appropriate documentation (amounts, FX rate, date and transaction details)	pr/di/de	a/m
					- establishing guidelines for the recognition and valuation of Bitcoin transactions	pr/di	m
					- hiring a professional (external) advisor	pr/di	m
					- manual review of transactions/ paid taxes	pr/de/cr	m
		KYC/AML Risks	2.28	2.95	- additional KYC check/identification of customer as part of the ordering process	pr/de	a/m
					- reporting of suspicious customers	di/de	a/m
					- internal assignment/mapping of public addresses to (real) customers	di/de	a
					- establishing an internal IT forensic division	pr/de/cr	a/m
					- using data analysis tools to detect unusual transactions	de	a
					- monitoring of applicable national regulation and if necessary implementation of the relevant actions	pr/di	m

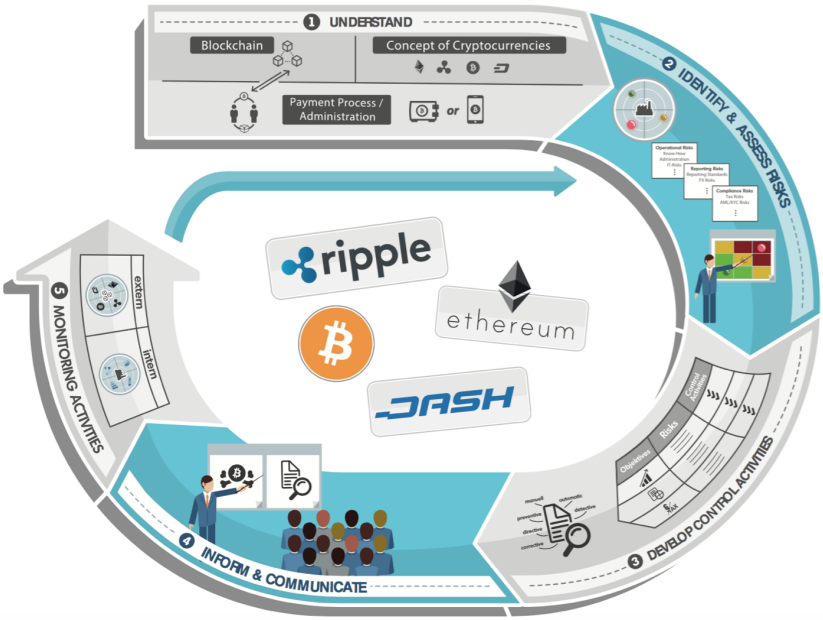


Figure 23: Cryptocurrency IC Framework; Source: Own illustration on the basis of the COSO 2013 IC Framework

incoming funds, such as hot or cold storage methods. Since cryptocurrencies are based on a new technology that has no other existing counterpart, a lack of knowledge would certainly aggravate every potential risk. Hence, it is imperative for a company to understand what a cryptocurrency is and how to deal with it in order to develop and further implement an appropriate risk management approach for its operational dealings.

2. Identify & Assess: In the second step, the potential risks that might emerge from the implementation of the new payment method have to be identified. For the risk identification process of cryptocurrencies, all potential threats that could influence the operational, reporting, and compliance objectives need to be analyzed and summarized (cf. the identified risks related to cryptocurrencies in Chapter 4.1). This process is continuous and not one-time because of ongoing changes in the company environment. However, when this process is "completed," the subsequent risk evaluation begins, which can be done by means of a risk assessment (cf. Chapter 4.2). By evaluating the risks previously identified according to their probability and severity, the risk assessment helps to determine the greatest risks.
3. Develop Control Activities: Thereafter, appropriate control activities have to be developed to mitigate the risks, particularly the most harmful ones, and these then need to be implemented. In this context, a risk control matrix (cf. Chapter 4.3.1) is a useful tool to help achieve this as it increases the transparency for all stakeholders and enhances their risk awareness, which in turn supports the process of developing control activities addressing the risks identified. These control activities may vary in terms of their form (preventive, directive, detective, or corrective) and type (automatic or manual). In the case of cryptocurrencies, it is more reasonable to focus on automatic, preventive, and directive control activities due to the irreversibility of transactions and the resulting irrevocable losses.
4. Inform & Communicate: Nevertheless, it is not enough to simply implement an effective internal control system because the controls also have to be correctly applied and executed. Therefore, when the control activities are implemented, appropriate information and communication within the company (across several business units) is also required. This particularly represents a problem in the context of cryptocurrencies because the most important information about this complex technology-based payment method has to be selected. Moreover, the necessary information needs to be prepared and communicated in a way that any employee is able to comprehend the payment method, the risks associated, and the necessary measures needed to mitigate them.
5. Monitoring Activities: Monitoring plays a significant role in ensuring that the controls implemented are efficient and effective. This implies that internal measures like guidelines, demarcated responsibilities, etc., have to be monitored and, if necessary, adapted. Furthermore, the external environment (e.g., the emergence of new cryptocurrencies, changes in blockchain technology, new regulations, etc.) should also be continuously screened so as to identify newly emerging risk factors. If there are any changes or new risks recognized, the company needs to conduct a renewed risk assessment, which means that the circle will start anew.

The established Cryptocurrency IC Framework, such as the COSO 2013 IC Framework, serves as a tool for an organization's management to develop a reasonable internal control (system), particularly with regard using cryptocurrencies as a payment method. The framework, however, does need to be adjusted and adapted to the particular conditions of each company, such as its size, regulatory environment, or the share of Bitcoin payments. Also, one must always take into account that the framework increases the likelihood of the company achieving its objectives, but it gives no absolute assurance that the goals will be definitely accomplished or that the emerging risks of accepting Bitcoin funds will be completely eliminated.

5. Conclusion

5.1. Summary of results

The literature review shows that the implementation of cryptocurrencies has led to the emergence of new risks that might affect a company's operational effectiveness, reporting objectives, and compliance regulations. Due to this, its operational effectiveness could suffer from a lack of know-how, a segregation of duties concerning the administration of Bitcoin funds, IT-related risks, and issues like the irreversibility of transactions. The reporting objective might be affected by the various national reporting standards and the resultant misrepresentation of financial statements but also due to the considerable FX risk of bitcoins received. Further, the compliance objectives could be influenced by issues related to tax-compliance, AML, and KYC.

By confronting companies that accept Bitcoin payments with these risks, it could be determined that their risk awareness and the corresponding evaluation of the risks proposed is quite poor. Risks related to FX are currently experienced as the most significant, and cyber risks are also considered as serious threats. The administration of Bitcoin plays an important role here as both risks are highly interrelated, for instance, private key storage depends on the (internal IT-related) storage option chosen. In contrast, the irreversibility of transactions and emerging tax risks are less regarded as threats for the operational dealing of cryptocurrencies. Moreover, the analysis revealed that methods to deal with the risks of cryptocurrencies are not yet firmly established, and many corporations had a significant lack of know-how in this regard. This can be seen in the fact that less than half (46%) of the participating companies have implemented internal controls, and around 29% do not recognize a segregation of duties as a risk so as to ensure appropriate risk management concerning the operational dealing of cryptocurrencies.

Nevertheless, a majority of the companies (46%) using internal controls have implemented, presented effective control activities to mitigate the potential risks identified. On the basis of the results obtained through this study, the author has developed a feasible concept that can be further adapted and supplemented depending on each organization's size, risk complexity, and additional changes in the cryptocurrency environment. By considering the Cryptocurrency IC Framework in combination with the integrated risk control matrix, an effective approach is proposed, aimed at ensuring the proper handling of cryptocurrencies and increasing the likelihood of an organization achieving its operational, reporting, and compliance objectives.

5.2. Discussion

The findings demonstrate that new, unequivocal risks emerge through the implementation of cryptocurrencies as a payment method, which can be due, on the one hand, to the properties of cryptocurrencies and on the other hand, to their underlying technology– the blockchain. However, the risks presented in this study may not be considered as a definitive list of all threats that might ever arise from using cryptocurrencies. In today's dynamic environment, a company must adapt to its environment, which requires the continuous monitoring and identification of newly emerging risks (Rüegg-Stürm and Grand, 2015, p. 78).

In general, the empirical analysis presented in this paper leads us to believe that companies do recognize these risks but only to a limited degree. Of course, only a small part of payments today are made using Bitcoin. This could be due to insufficient knowledge about the implementation of Bitcoin as a payment method but could also be due to its considerable increase in value during the last twelve months, which has made the cryptocurrency more attractive as a form of investment rather than a medium of exchange (cf. Appendix 2). However, as the share of crypto payments increases, its risk potential and severity evaluation will also become more important, because Bitcoin payments gain importance as their share in a company's total revenue increases. A logical implication of this is that the risk management involved in its operational dealing also becomes more important.

With regard to the risk awareness and risk assessment conducted, the FX risk was considered as the most important threat. One must mention that this risk might be completely eliminated by means of a payment processor and the immediate exchange into the relevant national currency. At first glance, the involvement of a merchant service provider simplifies the acceptance of Bitcoin payments and, moreover, several risks are already covered, such as the FX risk, the risk of payments defaulting, and, sometimes, KYC-related issues as well. Nevertheless, it is difficult to strike a balance between the advantages and disadvantages of a third-party provider because of the issue of third-party reliability and the processing fee per transaction. In this context, Massachusetts Institute of Technology's Professor Michael A. Cusumano (2014, p. 24) states that „payment processors and wallet firms are critical intermediaries and have also raised a lot of venture capital."

This statement indirectly introduces the second most significant risk, i.e., cyber risks, and the interrelated risk of the storage of bitcoins. Appropriate IT infrastructure and corresponding cyber security standards are critical for companies nowadays, especially in consideration of the storage of confidential data. As previously mentioned by Grant and Hogan (2015, p. 32), bitcoins are digital files "with a cash value

in the hands of the individual in possession of the file" or the corresponding private key. However, it is still difficult to limit the storage to the cold storage option because of the potential threat of the files being stolen by hackers. Cold storage also has drawbacks due to its physical nature. The recommendation of Sharma (2017, 14 November) and Antonopoulos (2015, p. 237), storing larger amounts of cryptocurrency assets on cold wallets and using hot wallets for day-to-day operations, seems reasonable. In this way, operational effectiveness could be improved and risks would be better diversified.

Independent of whether hot or cold storage method is chosen, it is important that the administration of Bitcoin payments is properly addressed. This can be done by limiting the access rights (to the private key or a hot wallet's password) to a small group of persons by assigning the responsibilities to those with the appropriate competence. Our findings indicate that, on average, two employees have the right to access this information, which seems appropriate, but one has to take into consideration that this analysis is mainly based on micro- and small-businesses and the results may differ in case of larger companies. Yet, there is no doubt that the field of competency should be assigned to someone within the senior management, preferably to someone who also has a high level of IT knowledge, like a CDO or CTO.

Apart from the fact that the risks are evaluated as somewhat low, the results of this study also indicate that there are currently a few companies with a significant lack of knowledge about cryptocurrencies. This became apparent in the respondents' answers like "I do not know where the company's bitcoins are stored" and "Everybody, or an intern, has the responsibility and access rights to manage the company's wallet." Additionally, the superficial risk evaluation considering the non-usage of a payment processor raises further issues. The answers show that the FX risk is considered as a threat by approx. 46% of the participants, so why do they not implement a payment processor that might mitigate this risk?

The last part of the analysis shows that the risks involved in dealing with cryptocurrencies are generally not yet firmly established because only around 46% of the companies claimed to have implemented internal controls in order ensure their proper dealing. It is even more alarming that approx. 10% of the participants were not able to assess the compliance risks related to Bitcoin payments, and about 20% could not evaluate if the development of internal controls is possible in this regard. These findings support the assumption that there is an important lack of know-how within organizations.

5.3. Limitations & Suggestions for Future Research

Notwithstanding the results presented in the previous chapters, there are some limitations to this study.

To begin with, how cryptocurrencies and their usage as a payment method will evolve and develop cannot be anticipated. This is because today's environment is highly dynamic and constantly changing, so that it is almost impossible to determine concrete rules and regulations to control a disruptive technology like the blockchain. Therefore, the results and the implied recommendations of this study are limited to the current status quo.

Second, the representative nature of this study is limited due to the selected sample, which mainly consists of micro- and small-businesses and thus does not represent the entire population (Brace, 2013, p. 7). This means that the results may differ for larger companies that have more complex structures that have a considerable impact on the assigned responsibilities and the related segregation of duties concerning the administration of Bitcoin funds within a company.

Furthermore, since Bitcoin payments currently only account for a small share of payments, it is important to note that the results of a risk awareness and evaluation may differ in the future. When the share of Bitcoin payments increases, it would also be required to conduct a more diligent reflection of the involvement of payment processors and the related costs and inherent exchange provider risks. The storage of Bitcoins will especially play an increasingly important role in this context. In addition, larger corporations located across several countries will be faced with the question of how to handle intercompany Bitcoin transfers because of differing national regulations and bans.

The scope of this study leaves open several options for future research. For instance, given the criticism of Bitcoin as a medium of exchange, future research could analyze cryptocurrencies that are a more appropriate fit as a medium of exchange, such as the zero-knowledge cryptography-based "Zcash" or the cryptocurrency "Ripple." The results of such studies could be used to adapt, specify, and supplement the Cryptocurrency IC Framework and the corresponding risk control matrix proposed.

Future studies could also adopt the opposite point of view by determining the general properties that any cryptocurrency should have in order to serve as an appropriate medium of exchange and, in particular, which risks should be addressed in the early stages of its development so as to prevent potential threats like how to make it a more secure medium of exchange.

References

Antonopoulos, A. M. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2015.

Arwinge, O. *Internal control: A study of concept and themes*. Springer Science & Business Media, 2012.

Azzara, C. V. *Questionnaire design for business research: Beyond linear thinking-an interactive approach*. Tate Publishing, 2010.

Bank for International Settlement [BIS]. Digital currencies [report], 2015. URL https://www.bis.org/cpmi/publ/d137.htm.

Berschens, R., J., H., and Holtermann, F. Kampf um den Bitcoin, 2017, 19. December. URL http://www.handelsblatt.com/my/finanzen/maerkte/devisen-rohstoffe/regulierung-der-digitalwaehrung-kampf-um-den-bitcoin/20742374.html.

Bhaskar, N. D. and Chuen, D. L. K. Bitcoin mining technology. In *Handbook of Digital Currency*, pages 45–65. Elsevier, 2015.

Bitcoin Foundation. Developers, 2017. URL https://bitcoinfoundation.org/developers/.

Blasius, J. and Baur, N. *Handbuch Methoden der empirischen Sozialforschung*. Springer, 2014.

Blockchain. Transactions per Day, 2018, 20. January. URL https://blockchain.info.

Böhme, R., Christin, N., Edelman, B., and Moore, T. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2):213–238, 2015.

Brace, I. Questionnaire design. how to plan, structure and write survey material for effective market research. London: Kogan Page Ltd., 2013.

BTC Echo. Bitcoin-Aktzeptanzstellen, 2017. URL https://www.btc-echo.de/bitcoin-akzeptanzstellen.

Buber, R. and Holzmüller, H. H. Qualitative Marktforschung: Konzepte-Methoden-Analysen, 2. *Aufl., Wiesbaden*, 2009.

Bungartz, O. *Interne Kontrollsysteme (IKS): Basiswissen für den Aufsichtsrat*. Erich Schmidt Verlag GmbH & Company, 2017.

Casari, E. Internal Control and Fraud Prevention (Master's Thesis, University of St. Gallen), 2017. URL http://www1.unisg.ch/org/biblio/edoc.nsf/SysLkpByIdentifier/10608826102/$FILE/10608826102.pdf.

Central Intelligence Agency. The World Factbook - Country Comparison: Stock of Narrow Money, 2018. URL https://www.cia.gov/library/publications/the-world-factbook/rankorder/2214rank.html#rs.

Choo, K.-K. R. Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In *Handbook of digital currency*, pages 283–307. Elsevier, 2015.

Cohen, E. The Bitcoin Economy. *Business NH Magazine*, 31(6):18–19, 2014.

Coinbase. Accept Bitcoin Payments, 2018, 12. February. URL https://www.coinbase.com/merchants.

Coindesk. Bitcoin Price Index, 2018, 20. January. URL Retrievedfromhttp://www.coindesk.com/price/.

Coinmap. Coinmap.org, 2017, 21. September. URL https://coinmap.org/#/world/48.09275716/3.73535156/5.

Coinmap. Coinmap.org, 2018, 5. January. URL https://coinmap.org/#/world/48.09275716/3.73535156/5.

Coinmarketcap. CryptoCurrency Market Capitalizations, 2018, 20. January. URL https://coinmarketcap.com.

Coinmarketcap. CryptoCurrency Market Capitalizations, 2018, 4. February. URL https://coinmarketcap.com.

COSO, C. o. S. O. o. t. T. C. Enterprise Risk Management - Integrated Framework. Executive Summary, 2004. URL https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf.

COSO, C. o. S. O. o. t. T. C. Leveraging COSO across the three lines of defense, 2013. URL https://www.coso.org/Documents/COSO-2015-3LOD.pdf.

COSO, C. o. S. O. o. t. T. C. Internal Control – Integrated Framework. Executive Summary, 2015. URL https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf.

Cusumano, M. A. The bitcoin ecosystem. *Communications of the ACM*, 57 (10):22–24, 2014.

de Jong, I. The role of virtual currency schemes in the modernisation of retail payments. *Journal of Payments Strategy & Systems*, 8(4):415–425, 2015.

Deloitte. Vorstellung der Blockchain-Technologie, 2016. URL https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Vorstellung%20der%20Blockchain-Technologie.pdf.

Di Pierro, M. What is the blockchain? *Computing in Science & Engineering*, 19(5):92–95, 2017.

Dombrowski, E. Analysis of bitcoin as a viable currency, 2014. URL http://www1.unisg.ch/org/biblio/edoc.nsf/SysLkpByIdentifier/10603116101/$FILE/10603116101.pdf.

ECB, E. Virtual currency schemes, 2012. URL https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

Elo, S. and Kyngäs, H. The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1):107–115, 2008.

Flick, U. Triangulation. Eine Einführung. 3., aktualisierte Auflage, 2011.

Franco, P. *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons, 2014.

Gautham. Japan Officially Recognises Bitcoin as Currency Starting April 2017. NewsBTC, 2017. URL http://www.newsbtc.com/2017/04/02/japan-officially-recognises-bitcoin-currency-starting-april-2017/.

Gisler, M. *Virtuelle Währungen-Eine ökonomische und finanzmarktrechtliche Einordnung am Beispiel Bitcoin*. PhD thesis, Universität St. Gallen, 2015. URL http://www1.unisg.ch/org/biblio/edoc.nsf/SysLkpByIdentifier/08604548102/$FILE/08604548102.pdf.

Goldman Sachs. Blockchain – Putting Theory into Practice [Equity Research Report], 2016. URL https://www.reddit.com/r/BlockChain/comments/58xf3q/goldman_sachs_report_may_2016_blockchain_putting/.

Graham, L. *Internal control audit and compliance: documentation and testing under the new coso framework*. John Wiley & Sons, 2015.

Grant, G. and Hogan, R. Bitcoin: Risks and controls. *Journal of Corporate Accounting & Finance*, 26(5):29–35, 2015.

Greene, C. and Shy, O. E-cash and virtual currency as alternative payment methods. *Journal of Payments Strategy & Systems*, 8(3):274–288, 2014.

Heer, C. Bilanzierung von Bitcoins, 2014, 10. December. URL https://www.wadsack.ch/news/datum/bilanzierung-von-bitcoins/.

Hern, A. A history of bitcoin hacks. The Guardian, 2014, 18. March. URL https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency.

Hoelscher, J. L. Digital currency risks: internal auditors need to advise management on the myriad risks posed by new forms of payments. *Internal Auditor*, 71(4):24–26, 2014.

Hunziker, S. *Erfolg der Internal Control-Eine empirische Analyse aus Sicht des Managements*. PhD thesis, Dissertation, Universität St. Gallen, St. Gallen, 2015.

IMF, I. Virtual Currencies and Beyond: Initial Considerations, 2016. URL https://www.imf.org/en/Publications/WP/Issues/2017/03/27/The-Macroeconomics-of-De-Cashing-44768.

IMF, I. The Macroeconomics of De-cashing, 2017. URL https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

Kanton, Z. Kryptowährungen (Bitcoin, Ethereum, Tokens usw.) [Merkblatt Steuern für Privatpersonen], 2017. URL https://www.zg.ch/behoerden/finanzdirektion/steuerverwaltung/kryptowaehrungen.

Kollewe, J. Bitcoin: UK and EU plan crackdown amid crime and tax evasion fears. The Guardian, 2017, 4. December. URL https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity.

Lam, J. *Enterprise risk management: from incentives to controls*. John Wiley & Sons, 2014.

Lindner, T. and Meyer, S. D. Besteuerung und Bilanzierung von Bitcoin. Rechnungswesen & Controlling, Heft 4/2017, 28-29, 2017.

Lloyds. Emerging Risk Report 2015 – Technology: Bitcoin, 2015. URL https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bitcoin.

Morettini, P. Does Blockchain Fit in Your Technology Stack?, n.D. URL https://www.pjmconsult.com/index.php/2018/01/blockchain-technology-stack-software.html.

Nakamoto, S. A Peer-to-Peer Electronic Cash System, 2008. URL https://bitcoin.org/bitcoin.pdf.

Nguyen, J. The Risks of Segregated Witness: Problems under Electronic Contract and Evidence Laws. *Computer & Internet Lawyer*, 34(11):1–8, 2017.

Nian, L. P. and Chuen, D. L. K. Introduction to bitcoin. In *Handbook of Digital*

Currency, pages 5–30. Elsevier, 2015.

Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. Blockchain. *Business & Information Systems Engineering*, 59(3):183–187, 2017.

of Internal Auditors (IIA), I. The three lines of defense in effective risk management and control. *Position paper*, 2013.

Papadopoulos, G. Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies. In *Handbook of Digital Currency*, pages 153–172. Elsevier, 2015.

Pfaff, D. and Ruud, T. F. Schweizer Leitfaden zum internen Kontrollsystem (IKS). *Verlag: Orell Fuessli. Switzerland*, 2013.

Piller, F. Virtuelle Währungen - Reale Rechtsprobleme? Eine zivil-, zwangsvollstreckungs- und steuerrechtliche Untersuchung aus der Sicht der Bitcoin-Nutzer, 2017. URL http://www1.unisg.ch/org/biblio/edoc.nsf/SysLkpByIdentifier/12608618102/$FILE/12608618102.pdf.

Rouse, M. Database (db), 2017. URL http://searchsqlserver.techtarget.com/definition/database.

Rüegg-Stürm, J. and Grand, S. *Das St. Galler Management-Modell*. Bern: Haupt, 2015.

Ruud, F. and Jenal, L. Licht im Internal Control-Dschungel. *Der Schweizer Treuhänder*, 79(6-7):455–460, 2005.

Ruud, F., Isufi, S., and Friebe, P. Pflicht zur Prüfung der Existenz des Internen Kontrollsystems: Bestandesaufnahme zur Steuerung und Kontrolle mittelgrosser Unternehmen in der Schweiz. *Der Schweizer Treuhänder*, 82(11):938–942, 2008.

Schmidt, T. Kryptowährungen und Steuern: Was jetzt wichtig wird. BTC-Echo, 2018, 18. January. URL https://www.btc-echo.de/kryptowaehrungen-und-steuern-was-jetzt-wichtig-wird/.

Sharma, T. K. Hot wallet vs cold wallet. The Blockchain Council, 2017, 14 November. URL https://www.blockchain-council.org/cryptocurrency/hot-wallet-vs-cold-wallet/.

Sixt, E. Bitcoins und andere dezentrale Transaktionssysteme. *Blockchains als Basis einer Kryptoökonomie, Wiesbaden: Springer*, 2017.

Sue, V. M. and Ritter, L. A. Conducting online surveys. Thousand Oaks, CA: SAGE Publications Ltd. 2007.

Swan, M. Blockchain. blueprint for a new economy: Beijing: O'Reilly, 2015.

Tindell, K. Geeks Love The Bitcoin Phenomenon Like They Loved The Internet In 1995. Business Insider, 2013, 5. March. URL http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4?IR=T.

Underwood, S. Blockchain beyond bitcoin. *Communications of the ACM*, 59 (11):15–17, 2016.

United States Treasury Inspector General for Tax Administration (TIGTA). As the Use of Virtual Currencies in Taxable Transactions Becomes More Common Additional Actions Are Needed to Ensure Taxpayer Compliance [report], 2016. URL https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf.

Vigna, P. and Casey, M. The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order: New York: Picador, 2016.

Westerhausen, H.-U. Das COSO-Modell: bisher nur eine Randerscheinung in Deutschland? Ein 13 Jahre altes IKS-Modell und seine Verbreitung in Deutschland. *Zeitschrift Interne Revision*, (3):98–103, 2005.

Worldcoinindex. Overview, 2018, 9. February. URL https://www.worldcoinindex.com/trending/overview.