Jani Kuusisto

CRYPTOCURRENCY IN PUBLIC AND COMMERCIAL ENTITIES

Financial risk and valuation

Faculty of Management and Business
Master's thesis
December 2021
Supervisor: Lasse Oulasvirta

ABSTRACT

University of Tampere, Faculty of Management and Business
Administrative sciences, public financial management
Author: KUUSISTO, JANI

Title: Cryptocurrency in public and commercial entities – financial risk and valuation
Thesis: 73 pages
Date: December 2021
Keywords: crypto, financial risk, accounting standards, valuation, balance sheet, systematic literature review, case study

---

Cryptocurrencies, such as bitcoin, have received extensive public attention. Cryptocurrencies are digital assets built on blockchain technology and openly traded on online exchange platforms. The cryptocurrency market´s rapid growth has encouraged corporate and governmental entities to trade and utilize cryptocurrencies.

Appearance of bitcoins and other cryptocurrencies in annual reports has created a need for new accounting guidelines addressing presentation and valuation of cryptocurrencies. This study intends to find out how different accounting standards address this need.

Risks are central to valuation of crypto assets. The study explores the cryptocurrency risks through the concept of financial risk, which is the sum of different risk dimensions perceived in cryptocurrencies. The goal is to figure out whether new risks have appeared by finding an intersection between academic literature and organizational reporting. Findings will reveal whether cryptocurrency risks have increased or decreased.

The study found out that there is some degree of consensus on valuation of cryptocurrencies as commodities in international accounting standards and annual reports of private companies. Presentation styles vary widely, but there were similarities in the valuation of cryptocurrencies across companies. Impairment testing was used to determine the fair value of cryptocurrencies in the companies. While the testing method was the same, the companies differed on their purposes for using cryptocurrencies, which led them to emphasize different accounting standards depending on the use.

While the corporate world and the governments are starting to use cryptocurrencies, it exposes them to new kind of risks that were left to less attention in pre-2018 academic literature. While some regulation has been enacted, lack of regulation and uncertainty how cryptocurrencies will be regulated remains a risk both in the academic literature and in the annual reports of the companies.

Applicability of international accounting standards on cryptocurrencies is still being actively worked on. There are still many gaps in the cryptocurrency risk literature. The academic literature seems to lag behind the corporate world in its discovery and analysis of the most relevant cryptocurrency risks. Cryptocurrencies are being innovated at rapid rate, which entails investigation in organizations using cryptocurrencies to receive the most updated perspective on the field.

Contents

List of figures and tables

1. INTRODUCTION

In September 2021, the country of El Salvador rose to headlines due to its adoption of Bitcoin as legal tender. El Salvador is the first country in the world to adopt a cryptocurrency for payments. The adoption did not start as well as expected. There were issues related to the government-supported bitcoin application, such as limited availability, technical glitches and even disappearance of bitcoins of the users. President Nayib Bukele promised $30 worth of bitcoin for each citizen who starts to use Bitcoin. (Reuters, 2021.)

In the light of COVID-19 pandemic, there has been a significant increase in the utilization of digital platforms to handle finances. Commercial organizations around the world are starting to use cryptoassets for making payments and investments. Blockchain is used to process digital transactions and it has gained more attention over time because of its high security. It is a new territory in the transactional landscape which means there can be both risks and benefits in using such a system.

This has raised the problems of valuation and ambiguous interpretation in accounting. Bitcoin has started to appear in annual reports of companies planning to invest, use or utilize bitcoin in other ways. The international accounting standards and documents from regulatory bodies and relevant entities are examined to find what is being discussed or instructed about bitcoin.

Different entities possess and use cryptocurrencies in different ways and for varying reasons. For this reason, the entities might report cryptocurrencies differently in their balance sheets and annual reports. The plan of the study is to find out whether the companies are following international accounting standards to the extent they have instructed how cryptocurrency should be handled.

This paper dives into Bitcoin´s utility for corporate and public organizations, from the perspective of financial risk and its valuation. To utilize crypto tokens in organizational activity, it is important to understand how it is valued in the balance sheet. The knowledge of valuation and financial risk provides clarity that is needed for proper handling on cryptocurrencies in financial statements. Studying financial risk of cryptocurrencies can provide more clarity on how risks should be considered in presentation and valuation of cryptocurrencies

Main concern with cryptocurrencies seems to be the risks associated with it. Because the risks play so pivotal role in understanding their value, this study will investigate risks in addition to valuation. There are different views on the concepts of risks associated with cryptocurrencies, which signals a need for clearer definition of risks in the cryptocurrency ecosystem. My intention is to choose a fitting definition for a risk when there is no academic consensus on it.

There are thousands of cryptocurrencies, therefore I am mainly focusing on bitcoin. Bitcoin is the most popular and known cryptocurrency, which makes studying it easier. In the theoretical framework I am going to describe Ethereum as well, which is the second largest cryptocurrency at the time of writing this paper. Many mainstream cryptocurrencies are based off Bitcoin and Ethereum, and that is why I deem necessary to include a brief description of Ethereum as well. I see it reasonable to describe basic technical aspects of these blockchains, as I do not think that describing only economic aspects would give adequate understanding of decentralized cryptocurrencies.

Both cryptocurrencies are using blockchain technology to make their decentralized governance possible. This brings new risks and possibilities, and the study is going to examine risks concerning blockchains that can affect possible financial and operational activities of entities. Blockchain technology provides a digitally distributed, decentralized and public ledger which records cryptocurrency transactions.

The blockchain technology behind the cryptocurrencies is being innovated constantly and there is tremendous lack of research literature covering the topic at the time of this study. There has recently been an outflow of academic research focusing on cryptocurrencies, and this study attempts to aim at better understanding of the risks by analysing academic literature.

2. THEORETICAL FRAMEWORK

2.1 Blockchain technology as innovative cornerstone

If looking at timeframe from 2008 to 2015, investment in financial technologies globally increased by more than 2.200% from $930 million to $22 billion. And then it nearly doubled from 2015 to 2017 by $40 billion. “Financial technology” is also abbreviated as “FinTech”. Financial innovation itself has a long history that can be presumed to have started in 1866 when the first transatlantic cable allowed the utilization of technology in finance. Smartphone and application programming interfaces (APIs) drove financial innovation further and the financial crisis in 2008 accelerated the development of it. FinTech can be categorized in three different eras. FinTech 1.0 (1866-1967), FinTech 2.0 (1967-2008) and FinTech 3.0 (2008-). Currently, FinTech 3.5 can be said to exist in emerging markets, otherwise developed countries are categorized to be in FinTech 3.0. (Weiyi 2018, 965-966.)

2.1.1 Bitcoin – the most well known blockchain

According to Satoshi Nakamoto´s whitepaper, bitcoin can be defined as a type of electronic cash that can be sent online with out the need of a financial institution as an intermediary. Bitcoin uses peer-to-peer networks to hash transaction into a chain of hash-based proof of work. This forms a record that can´t be changed and thus making a decentralized ledger of financial transactions possible. (Nakamoto 2018, 1.)

Transactions in Bitcoin are placed in to blocks, and these are chained together creating a history of transactions called blockchain.

Grover describes blockchain as a time-stamped ledger, that is public for all users, peer-validated and write-only. In the simplest terms, it is a data structure that holds transactional records while ensuring its security and visibility. When transactions happen, they come from a consensus making protocol. (Grover 2019, 735.)

The structure of Bitcoin´s blockchain can be understood as four different layers described by Eyal. The layer on the top can be called “the system clients”. This layer keeps track of account balances and has data on the number of coins in each account. The second layer is virtual machine layer, and it processes bitcoin transactions and translates them in to changes in system´ state. The other two layers are consensus protocol layer and network layer. These two layers co-ordinate the system´s state of large number of machines. (Eyal 2017, 39.)

These layers allow the possibility of using smart contracts. They also provide the necessary reliability and security that is missing from traditional way of transacting financially. As an example, companies can use smart contracts to provide securities that can be traded with out the need for additional supervision. Distributed-ledger technology can be used to send fiat currency and physical goods digitally. This technology can provide new opportunities, and bitcoin originally emerged as an alternative for traditional currencies that are controlled by a central entity. Invention of digital transaction is not new, and it posed significant risks. Problem with digital currency is that it is made of bits and can be copied. This lets someone to make money when they are not supposed to. This is the reason that such system must rely on a bank or similar entity to prevent the creation of illicit currency and authorize the users to sell or receive currency. Bitcoin can be used as an answer to this challenge, as it does not have to rely on anyone due to its distributed-ledger system that can function itself to execute orders and reliably keeping track of its users' legitimate funds. (Eyal 2017, 39-40.)

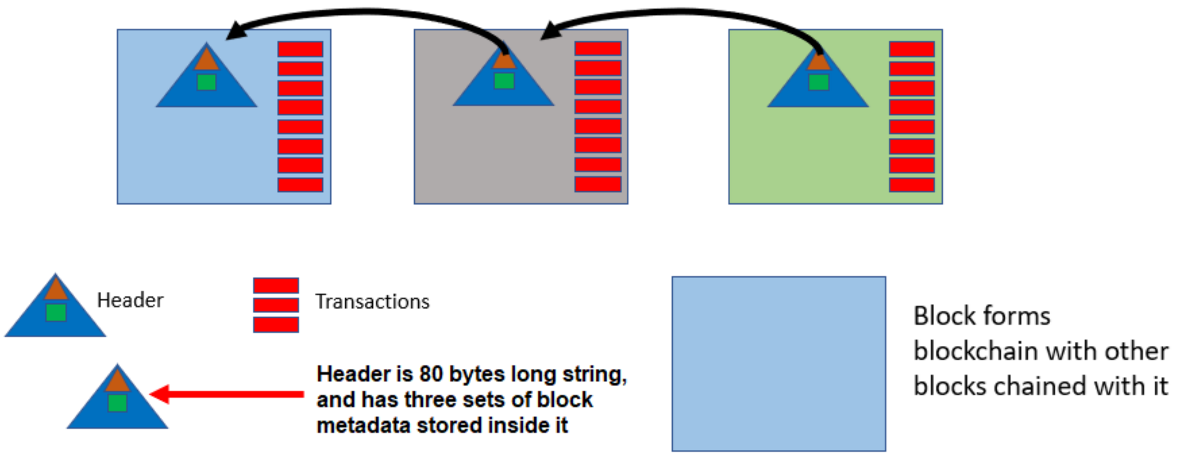

Figure 1. Functionality of blockchain. Each block is referenced by its preceding block, as shown in black arrows. Transactions are put inside the blocks. The header has the cryptographic puzzle. This puzzle has solution, which is shown as small green square in the figure.

In every block of the blockchain, there is a cryptographic puzzle inside. The miner must solve this puzzle to create a new block. This process of solving the puzzle takes resources from the miner to do it. This event where the miner must spend resources to solve each puzzle, is called proof of work.

The algorithm automatically changes the difficulty of the puzzle, so that new blocks are generated at controlled and stable intervals. Sometimes a fork might appear. This happens when a miner accidentally creates a separate block. Forks are not ideal for the blockchain, because they make additional branches which are not in order. (Eyal 2017, 40-41.)

The main rule in a situation like that is the longer branch is the main branch and thus the only valid branch. Blocks in the shorter branch are weeded out and any transactions in them are invalidated. If a fork appears, the branch which miners choose becomes longer and this is how the state of the blockchain is kept under control. (Eyal 2017, 41.)

When talking about security of Bitcoin, it is important to remember that an attacker might try to create new forks to change the direction of the blockchain. This is prevented by the longest-chain rule. The chance success of an attack like that is very low, because the attacker would need to have more computational power in his computer than rest of the miners in total. If a branch has enough blocks following it, it will not be pruned. What also adds to the security, is the fact that users themselves can choose how many confirmations they want. (Eyal 2017, 41.)

Attacker has higher chance of success, if there are too many accidental forks created by other miners, because this results in the main branch expanding slower. For security reasons to prevent forks like that from appearing, the interval for creation of a new block is much longer than the time it takes for a new block to copy itself across the network. Intervals can´t be made too short and blocks can´t be made larger. Larger blocks would take longer time to copy itself. (Eyal 2017, 41.)

This is how the security of Bitcoin´s blockchain is organized and it can´t be tweaked to make new blocks very fast or make them too big. Bitcoin´s security is dependent on miner´s spending resources on the mining process which has raised the environmental discussion. This is a down-side with bitcoin and that is why there are many who have tried to make a solution to patch-up this inefficiency. (Eyal 2017, 41.)

One problem with Bitcoin has always been the waste that it produces. As Bitcoin´s value increases, miners need more computational power to create new blocks. This requires more and more power and leads up to unacceptable levels. Due to this reason, there are many alternative cryptocurrencies on the market which try to address this issue. (Eyal 2017, 45.)

There are also certain concerns about privacy when using this technology. On blockchain, it is possible to see transactions that happen between addresses. Everyone can see the transactions, which can be both a good and bad matter. For example, competing organizational entities might not want that a competitor sees their transactions that have taken place. While using blockchain does not directly compromise one´s identity, it is possible to pinpoint the identity by analyzing transactional data and gathering addresses that belong to the same entity. (Eyal 2017, 46.)

Some cryptocurrencies have tried to tackle this privacy issue. A technique called zero-knowledge proof is being used by Zcash to secure the identities of those who send transactions. How this works, is that instead of users sending transactions to each other´s public addresses like in Bitcoin, they send it to a shared public bucket that is used for everyone transacting in Zcash. There is a unique secret linked to each transaction that takes place. Proof of the secret is used by the receiver of the cash to request the Zcash in the bucket that was sent there from another address. (Eyal 2017, 47.)

While ZCash´s system would bring more privacy than Bitcoin´s, is it too much privacy? It is not certain if the FinTech industry needs this much privacy. It would create some complexity for auditing, insurance and banking and require some separate identification agreement between the client and the organization so that the necessary visibility is accomplished. This is where Bitcoin does not have as much similar problems when it comes to adopting the cryptocurrency for use like mentioned earlier. (Eyal 2017, 47.)

2.1.2 Blockchains and their utility for governments

Smart contracts are lines of programmed code that create the rules for the service that is using these contracts. Ethereum blockchain contains these smart contracts. Ethereum can be thought of as a technology environment in which decentralized smart contracts can be developed. The difference between Ethereum and bitcoin is that the blockchain Ethereum can be utilized in broader ways. Ethereum´s blockchain is specifically built for widely customized smart contracts.

The smart contract can be activated in two ways. It can be activated internally by other such contracts inside the blockchain or externally via transactions. Using Ethereum for these smart contracts require a fee. This fee is called gas, it can be paid in ether, which is the currency of Ethereum. Reasons to utilize smart contracts are numerous. Smart contracts can be used in voting systems, outsourced computation, option contract or decentralized gambling to name some examples. (Vinayak 2018, 1701.)

According to Vinayak, smart contract is an attractive target for attacks. Especially contracts which hold a specific amount of money are of great interest to attackers. When speaking about security vulnerabilities in smart contracts, malfunctioning or buggy code can result in unexpected activation of smart contracts. In addition to this, smart contracts are irreversible once they are published on the blockchain. That is why it is necessary to check the contract for vulnerabilities before its development.

Use of the blockchain technology in financial sector could result in significant savings estimated tens of billions of dollars. There is a lot of research surrounding the use of Ethereum and smart contracts in removing the need of centralized party. It is also argued that this new technology could reduce operational costs. (Vinayak 2018, 1702.)

Bitcoin and Ethereum are considered the largest cryptocurrencies because their market caps are the highest. As the writer of the paper, I think that these cryptocurrencies are the most essential for businesses and governments looking to get into the crypto space. Bitcoin is the oldest and most used cryptocurrency, referred to some as “digital gold”. Ethereum on the other hand has massive and complex ecosystem and is being used as a base for other cryptocurrencies. After describing these cryptocurrencies in detail, I will go through the adaptation of these cryptocurrencies in the monetary sector and in the government.

Global adoption of digital currencies would also raise risks in the monetary sector to some extent. If central banks have less influence over monetary policy because of digital currencies, they might not be able to positively influence economic growth by controlling inflation. On the other hand, sometimes central banks handle the feat currencies incorrectly, setting up the economy to move towards disaster. (De Filippi 2018, 70, 108.)

Some governments have been exploring the possibilities blockchains can bring for more effective governance. Sweden and the Republic of Georgia have strived towards progress to create systems based on blockchain technology, which store information on land ownership. More specifically, information on owners of different lands and the previous owners of these lands in the past. Each land title has its own token for it on the blockchain. And when this token changes owners, so changes the landowners as well. (De Filippi 2018, 109.)

This information is recorded on the blockchain, which stores this information permanently in a tamper-proof way. This way, there is reduced risk of corruption or loss of data. It also is more beneficial for landowners because it increases the security of their owned land; Blockchain keeps the record of who owns the land and cannot be changed even if the government is overthrown or alike happens that would compromise the ownership. (De Filippi 2018, 109.)

For more examples, the nation of Estonia is collaborating with BitNation to make notarization services that utilize blockchain. This would allow Estonian citizens to record all notary information, such as birth certificates, on a blockchain. Blockchains and smart contracts can be used to turn mortgage payments into securities. Government services can also be automatized to follow the data on blockchain. If there is a death, and the death is recorded to a blockchain, government services related to the death would automatically initiate. (De Filippi 2018, 110-111.)

Tokenization of property market could make the market as fast as Bitcoin transactions are. In such a market, you could buy a property on the other side of the planet in minutes. It would not matter whether you live right next to the property, or far away from it, the transaction times to buy property would be the same. Blockchains can also provide a safe database for sensitive information. Government can store hashes on the blockchain, which mark confidential information. Let´s say there is an attempt to modify records that have confidential information in them. If there is a file on the government´s files that has a hash differing from the hashes stored on the blockchain, this exception can be detected easily, and appropriate actions taken quickly. If there is an attempt to install malware into the government files, blockchain can provide a traceable trail that can lead to identification of the attacker. As a real example, the DARPA signed a deal with Guardtime for 1.8 million dollars to help them figure out a blockchain-based system for storing important military data. (De Filippi 2018, 111-112.)

The blockchain technology can be used to replace certifications and access control systems. If someone has committed a fraud for example and a government agent wants to pull up the record of the fraud, there is no need for the government agent to see the entire criminal record of the individual. With blockchain technology, a hash can be made of the fraud crime and this hash can be pulled from the blockchain so that the government agent would see if the individual had indeed committed a felony or not, but the agent would not see any other possible crimes on the record. This would grant the government agencies access to the information they need and reduce the additional unnecessary confidential information from being seen by different government workers. (De Filippi 2018, 113.)

Blockchains have vulnerabilities and are not immune from attacks. Depending on which mechanism the blockchain is relying on, there are different ways to manipulate it with an attack. Bitcoin uses proof of work consensus mechanism to verify transactions. To launch an attack that could modify or remove previous transactions in the blockchain, an attacker would need to form a 51% majority on the blockchain which would cost around one billion dollars. Of course, making such an attack is more useful for the attacker if the governments are using blockchains to store classified data.

Second and more convenient way of attacking would be to steal the government´s private key that is used to authenticate transactions. Then the attacker could use the key to add false records in the government´s name. The same problem occurs if a private individual loses their private key. It would prevent them from doing transactions on the blockchain. If there is data on the blockchain that is inaccurate or of low quality, it will not be fixed because there is nobody checking and ensuring the quality of the data on blockchain. It is missing a centralized party in charge of monitoring it. (De Filippi 2018, 113-114.)

Government registries using blockchain technology would need institutional support from the government to be possible. There must be a quality control and monitoring system, where there are clear assignments of responsibilities on who can store and view information on a government´s database. Also, some privacy risks might arise if government puts their records on a public blockchain. Anyone on the Internet could see the records there. An instance where a privacy problem could occur is that if someone collected data on someone´s owned lands from the blockchain, they could come up with accurate estimation of the person´s wealth. It could violate someone´s privacy who would not want that their amount of wealth is known. (De Filippi 2018, 115.)

The adoption of governmental blockchain databases could result in more transparent and reliable databases. Blockchain´s flaw is that it is very tamper-proof and that itself could reduce the effectiveness of governmental blockchain database. There are also some privacy risks associated with blockchains, which were mentioned earlier. At the time of writing, this technology is still new and more ways of using it in different contexts are being explored actively. (De Filippi 2018, 116.)

In the end, blockchains are maintained by programmers and miners. Miners are usually motivated by monetary incentives. They are also indirectly maintained by hardware manufacturers to some extent. People who maintain the blockchains can be regulated by laws and rules set by governments. There are many different forces that influence the people who maintain the blockchains. There are, as mentioned before, laws set by the government, but also social norms dictated by social groups, market forces and the architecture of the blockchain technology in general. (De Filippi 2018, 173.)

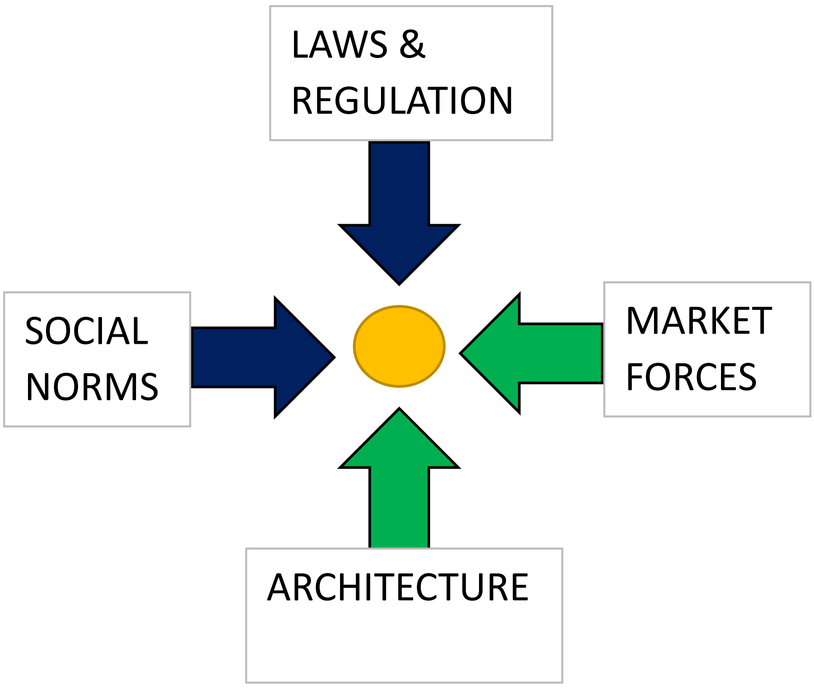

Figure 2. Four modes of regulation by Lawrence Lessig. The yellow circle in the centre is the actor maintaining the blockchain.

The modes of regulation can sometimes overlap. This is the case when government tries to influence the maintainer for example by creating a law that does not directly affect the blockchain and the maintainer but pressures the maintainer. If the government creates a law that forces the people participating the market to pay higher taxes, it will inevitably affect market forces and might change the architecture. Taxes can also be used to create social norms. It is important to keep in mind that even though government can affect the blockchain and its market in this way, the blockchain is still decentralized. That means, the government can´t directly change the basic operation or the principles underlying the blockchain. Therefore, the four modes of regulation might not have as strong effect in the end as originally intended. (De Filippi 2018, 174.)

In the four modes of regulation, I referenced the yellow circle in the middle to be a maintainer of the blockchain. However, it is important to acknowledge, that it might not even represent the maintainer in the reality. It is becoming less and less apparent, that there even is any kind of entity in the centre, because the code-based blockchain systems are operating autonomously. This makes it difficult for the government to target regulation specifically at any entity. It looks like the government could regulate the blockchains like it regulates the Internet. Instead of directly regulating blockchain, which is impossible, it can regulate its users, and anyone associated with it. The governments around the world are doing exactly this when they want to regulate the Internet. (De Filippi 2018, 174-175.)

The miners have centralized to work in mining pools for the purpose of computational power combination in hopes of achieving higher likelihood of achieving a block reward. It is estimated that 4 mining pools have majority control over the Bitcoin blockchain, and two mining pools have majority in the Ethereum blockchain. The power of these mining pools can demonstrate in the possibility that they could collaborate and fork the blockchain to another direction. (De Filippi 2018, 180.)

These mining pools could provide an opportunity for the government to use them for regulation purposes. The governments could push the mining pools to make changes to the protocol. Governments can use taxes and penalties to enforce laws and regulation on the mining pools. It is arguable how much effect the government could have on the mining pools, as the blockchain is global and decentralized. Change in the direction of blockchain requires network-wide consensus, and different groups of miners around the world could nullify the effect of government regulation on the blockchain. (De Filippi 2018, 180-181.)

Public sector organizations could work as miners and directly affect the blockchain through having the ability to vote with its mining station´s computing powers. They could also contribute to the development of the blockchains and work with other organizations to achieve their aims. (De Filippi 2018, 189.)

2.2 Financial risk in organizational use of cryptocurrency

Christoffersen describes financial risk as a broad concept that can be split into four different risk categories that are included in it. In the context of this paper, the financial risk is defined as possibility of losing money on an investment or other utilization of cryptocurrency. The financial risk occurs when any of its four sub-risks occur. Christoffersen describes the four sub-risks as follows:

1) Market risk: The market risk is related to how markets change the prices of interest rates, equities, and foreign exchange rates.
2) Liquidity risk: Occurs when the organization is unable to fulfil its short-term debt obligations and unable to organize enough funding in a specific timeframe. Especially the 2008 financial crisis increased attention to this before overlooked risk category.
3) Operational risk: A risk of loss due to human failure, technical failure, or other physical event in the organization. Managed through insurances.
4) Credit risk: Risk related to the other party not able to complete their obligations. The risk manifests if the other party is not able to pay back their obligation in the full, even if they pay it partly.

(Christoffersen 2011, 3–4.)

This breakdown of financial risk in to four different risks that form a financial risk provides suitable delimitation for the study. There are some cryptocurrency-specific considerations that needs to be made when observing the financial risk in the way mentioned earlier. For instance, in cryptocurrency, volatility is often large part of what forms a market risk. Credit risk as a concept is ambiguous and different researchers define it in different ways. That is the reason the definition of credit risk will be extended to mean any kind of risk posed by the counterparty. Christofferson's definition of liquidity risk will also be extended to mean risks against the total liquidity of crypto assets, caused for instance by legal grey areas and sudden liquidity changes in the environment. The definition of operational risk is accurate and does not need specific changes to match it to the context of cryptocurrency risks.

There has been little research on cryptocurrencies before the year of 2018, which is why I have taken newer research to supplement the theoretical framework, but only including research before the year of 2018 for the table (see table 2) that is used in the systematic literature review. After the year of 2018 the interest in cryptocurrencies exploded and vast research was conducted, but before there was much less research.

2.2.1 Market risks in crypto assets

The significance of cryptoassets has increased so much that IMF reported financial data related to the beneficial effects of crypto assets as a separate asset class (in IMF BOPCOM 18/11). (Ramlall 2019, 20.)

	Bitcoin	**S&P 500**	**Euro**	**Chinese Renminbi**	**Gold**
Bitcoin	1	0.02	-0.04	0.04	0.03
S&P 500	0.02	1	-0.05	-0.09	-0.14
Euro	-0.04	-0.05	1	-0.37	0.42
Chinese renminbi	0.04	-0.09	-0.37	1	-0.28
Gold	0.03	-0.14	0.42	-0.28	1

Table 1. Matrix of unconditional covariance of daily returns – correlation comparison between different assets, including cryptocurrency bitcoin. Table presentation from Ramlall and data from IMF.

According to the data above, there is seemingly little correlation between bitcoin and other asset classes. This could indicate that the risk that the crash of stock market or feat currency causing crypto asset bitcoin to decline is very low. If reflecting this correlation finding against market risk of using or investing in cryptocurrency bitcoin, it is a risk-reducing factor in this risk category.

Bitcoin is well known for its high volatility, and while its independence from significant correlation with other asset classes reduces market risk of using it, its high volatility is a strong factor that drives the market risk higher. Dyhrberg's analysis of Bitcoin´s volatility addresses the fact that Bitcoin is sensitive to certain shock and its behaviour imitates random walk behaviour. Sometimes Bitcoin has periods of high volatility, and sometimes it is stable and weak in volatility. Dyhrberg further asserts that this kind of behaviour is typical of financial assets. (Dyhrberg 2016, 87.)

Traditionally, financial institutions have taken measures to reduce the market risk with mitigation methods. In cryptocurrencies, these mitigation measures can be built inside the system in form of smart contracts. Paech states in his article, that there are two ways this can be done. These measures can be built inside one colossal network, or alternatively, several networks. Using one large network would raise a systematic risk and using several networks would make an extremely complex set-up raising a complexity risk and requiring additional work regarding interoperability. (Paech 2017, 16.)

2.2.2 Liquidity risk influenced by common trust and governments

The liquidity risk in this study will be examined from the perspective of cryptocurrencies and it is conceptualized in this study a little differently from how Christoffersen described it. Liquidity risk in the context of this paper is examined from the point of view of an entity´s crypto assets, which are under risk from sudden changes in liquidity caused by a third party such as a regulator or an exchange.

There have been some studies regarding using cryptocurrencies as a liquid investment asset. A study conducted by Othman, Abdullah and Haron examined whether cryptocurrencies are valid to be used as a liquid asset to reduce liquidity risk. It compared the characteristics of bitcoin cryptocurrency with requirements set in High-Quality Liquid Assets (HQLA) about the standards of Basel III. It also drew comparisons more specifically between the volatility structure of the assets recommended as HQLA and the bitcoin.

The study defines liquidity as an organization´s capability to fulfill its obligations, without significantly impacting its financial condition or day-to-day operations. The primary goal of liquidity risk management is described to ensure that the organization is handling their liquidity in a fashion that does not result in additional costs because of passing due dates or other losses. If liquidity risk is not taken care of, it can result in having to liquidate assets at prices that are lower than normal market sale prices, which can cause severe financial damage on the organization. Financial crisis between 2017 and 2018 brought some attention to liquidity risk. (Othman 2019, 108-109.)

Basel III standards state, that assets which can be converted into cash immediately and with relative ease can be HQLA assets. Two asset traits define whether an asset can be classified as a HQLA asset: Fundamental characteristics and market-related characteristics. Part of a liquid asset´s fundamental characteristic is its low risk. Low legal risk, low inflation risk coupled with high credit standing of its issuer, low subordination and low foreign exchange risk all make the asset more liquid. Speaking about credit ratings with cryptocurrencies, some rating agencies, like Weiss Ratings, have started to review credit ratings on cryptocurrencies since 2018. In 2019 the rating of bitcoin stood at B-, and none of the cryptocurrencies listed in the review exceeded the rating of B. Because the cryptocurrencies are decentralized, they have low degree of subordination. This gives them value that is difficult to dispute. (Othman 2019, 112.)

Jennifer Shasky Calvery the director of the Financial Crimes Enforcement Network forecasted that the bitcoin might turn out to be “a significant player” in the system of finance. There is acceptance for the blockchain technology underlying the crypto transactions, but many doubt the bitcoin itself. (Luther 2016, 397.)

The biggest reason why bitcoin is adopted on larger scale can be attributed to incumbent-monies problem. For bitcoin to be able to replace the traditional currencies, it must be so much better that it can justify the cost of switching currencies. Switching costs mean the costs which come in result of switching to another currency. These costs can come for example from the need to modify automatic teller machines, update transaction records and retooling vending machines (Luther 2016, 398.)

Government backed currencies also permit the government to make their own monetary policy, generate extra revenue and provide the government with ability to supervise and confiscate currency. Because bitcoin or other electronical currencies can conflict with governmental control, it can result in government taking actions against these currencies, such as discouraging its use or outright banning it with regulation. On the other hand, absence of regulation can reduce demand because it leaves a legal grey area which creates ambiguity. (Luther 2016, 399.)

The technological upside in bitcoin is its capability to handle transactions over distributed network without requiring a central node. In addition, it appears that processing transactions using the blockchain comes with less costs than the traditional way of processing transactions. A benefit in using cryptocurrencies illicitly can manifest if switching to cryptocurrency would enable the user to complete transactions that they would otherwise would not be able to send. For instance, it was the only method approved on the Silk Road, an online market for trading illegal goods. (Luther 2016, 401.)

Chinese authorities in 2014 raised concerns regarding the fact that online money market funds allow investors to withdraw their funds at any time, increasing liquidity risk. (Lin, Whinston & Fans 2015, 7). This might cause liquidity problems not only for the funds, but also exposes the market for sudden changes in liquidity of cryptoassets, making quick disappearance of large chunk of investor´s allocated funds possible as well.

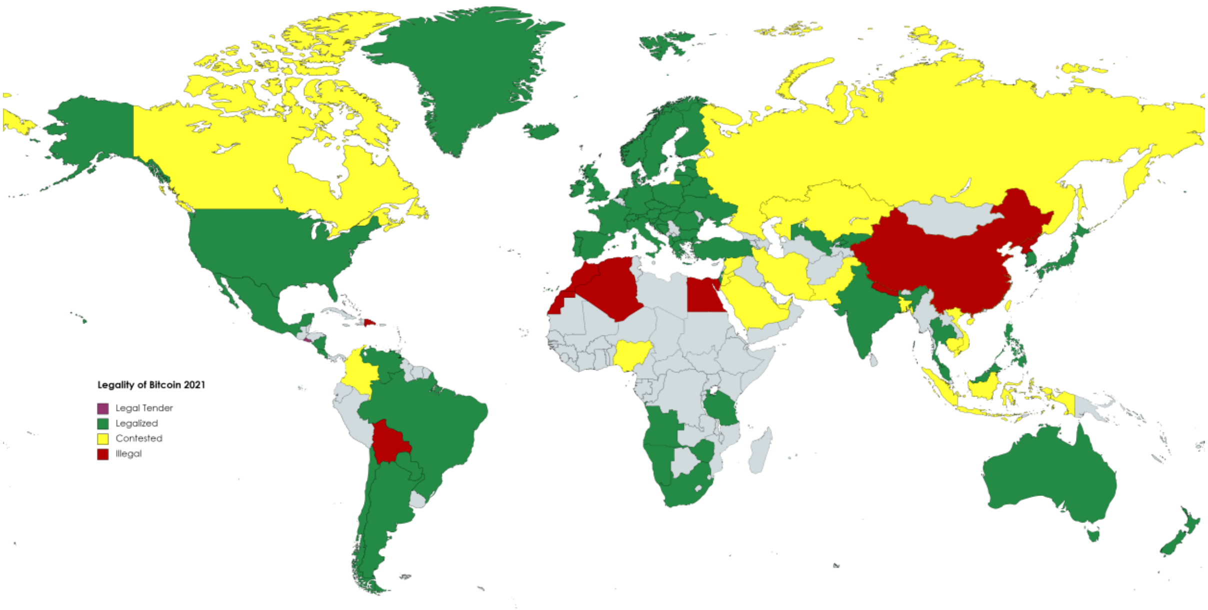

Figure 3. Status of bitcoin´s legalization in different countries. At the time of creating this map (September 2021), only El Salvador is using bitcoin as legal tender. Green stands for legalized, yellow for contested and red for illegal.

2.2.3 Operational risks with cryptocurrencies

“Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.” (Peters 2016, 241.)

As cryptocurrencies become more popular in the economies of countries and banking systems, operational risk becomes more significant risk factor. Operational risk manifests from time to time, such as when there was a famous case of Mt Gox losing 750 000 bitcoins to hackers. (Peters 2016, 242.)

Peters has separated different risk drivers that arise while using cryptocurrencies and placed them in further sub-categories of vulnerabilities and exposures. He also placed specific operational risks under different risk drivers and assigned a OR Basel category for the risks. His sheet also includes mitigating actions that can be done if a mitigated action is known to exist for an operational risk. (Peters 2016, 257.)

Decentralized governance of Bitcoin is mentioned as an operational risk because it relies on the CPU power of its honest nodes. As long as the honest nodes have more CPU power than the attackers, the system stays secure. Transactions in the system are validated through peer-to-peer network, where the nodes use CPU power as their validating power. (Peters 2016, 256.)

In the vulnerabilities, he listed decentralized governance, peer to peer verifications, irreversibility of transactions, anonymity, private key as unique mean of access and publication time gap. In the exposures he listed multiple jurisdictions, micropayments, hardware reliance and software reliance. More elaborately, he listed governance risk, abuse of power, price manipulation, fraud, price volatility and changes of protocols as operational risks that are driven by decentralized governance. (Peters 2016, 257.)

To mitigate risks that originate from decentralized governance, he proposed to codify network and governance powers in cryptocurrency related deposit banking services. In the risk driver peer to peer verifications, he listed an operational risk of double spending attacks. To mitigate this risk driver, he proposed to have high computational power. Transaction irreversibility is also listed as a risk driver, aggravated losses in case of errors on theft on private keys as operational risk for it and cyber security as a solution to mitigate that risk. The fourth risk driver he mentioned was anonymity. Operational risks related to it were money laundering, fraud, legal risk, and compliance. Forcing identification was given as a solution to mitigate this risk driver. (Peters 2016, 257.)

The article mentions that if the private details are stolen, the thief also gets to link the address of the owner with the owner´s identity. Because all the transactions of Bitcoin´s blockchain are public information, it would be possible to see the entire transaction history of a specific person once their identity is revealed. It would also reveal with whom the person transacted, when and how much bitcoins were transacted. To get around this issue, the article mentioned that it is possible to implement a system which changes address after every transaction that was executed. (Peters 2016, 263.)

The fifth risk driver was private key as unique means of access and its operational risks were external fraud, internal fraud, processing errors, damage to physical assets and attacks. To mitigate this risk driver, a risk mitigation technique identical to sensitive information handling in banks was required. The final and sixth risk driver in vulnerabilities category was publication time gap. Risks related to it were fraud in double spending, fake transactions, attacks, and transaction malleability. There was no action listed to mitigate this risk driver. (Peters 2016, 257.)

In the exposures risk category, there was multiple jurisdictions risk driver and operational risks caused by it were regulatory breach, tax avoidance and tax law compliance. Second risk driver in exposures category was micropayments and operational risks for it were internal fraud, external fraud, systems failure, process errors and reporting. The third and fourth risk drivers in the table were hardware reliance and software reliance. Operational risk for hardware reliance was exposure to hardware failures and for software reliance exposure to software failure. In software failure, it could drive an impact of data theft. For the exposures risk category, there were no mitigation actions mentioned to mitigate the risks. (Peters 2016, 257.)

2.2.4 Exchanges as point of view for credit risk

Moore´s and Christin´s empirical analysis of Bitcoin-exchange risk examined the credit risk related to cryptocurrency exchanges. The research analysed 40 different Bitcoin exchanges operating between the years 2010-2013. At the time of the study, 18 of the 40 exchanges had been closed and in many cases the customer account balances had disappeared too. The study used a model called proportional hazards model to figure out whether the exchange is likely to close strongly correlating with the exchange´s transaction volume. (Moore & Nicolas 2013, 25.)

Cryptocurrency exchanges encountered two kinds of risks in the study. One was the risk of security breach, which was more likely if the transaction volume was very high, and the other risk was premature shutdown of the exchange, negatively correlated by its transaction volume. (Moore & Nicholas 2013, 32) A security breach might result in large amounts of cryptocurrency being stolen from the exchange. The exchange operators might find it difficult to recover the stolen funds, if returning them is on the hacker´s discretion. If the exchange is shutdown prematurely, in that case it is not self-evident either, whether the customers will be funded their deposits. For instance, 11 out of 18 exchanges which closed reimbursed their customers in the study. (Moore & Nicholas 2013, 27.)

A research article written by Lin Zhangxi, Whinston B. Andrew, and Fan Shaokun explained different sources of credit risk in Internet finance. The platform of finance could pose a credit risk in form of its business model. As an example, the study discovered that some online finance platforms make the relationship of lenders and borrowers blurry, leaving an opportunity for the platform to take a cut from the investor´s funds. (Lin, Whinston & Shaokun 2015, 16). This study is well applicable when an entity wants to use interest generating service providers who lend the entity´s invested money to borrowers.

2.2.5 Financial risk framework

I have gathered risk discussing literature from the years of 2013-2017 into the table below. My purpose is to use this table as a framework for financial risk. This way the financial risk can be understood and studied further.

	Financial Risk		
Market risk	Liquidity risk	Credit risk	Operational risk
High volatility (Dyhrberg 2016)	Absence of regulation (Luther 2016)	Exchange shutdown (Moore & Nicolas 2013)	Decentralized governance (Peters 2016)
Systemic risk (Paech 2017)	Conflict with state control (Luther 2016)	Security breach (Moore & Nicholas 2013)	Peer to peer verifications (Peters 2016)
Systematic risk (Paech 2017)	Instant withdrawal (Lin, Whinston & Fans 2015)	Platform risk (Lin, Whinston & Fan 2015)	Transaction irreversibility (Peters 2016)
			Anonymity (Peters 2016)
			Private key as mean of access (Peters 2016)
			Publication time gap (Peters 2016)

Table 2. Financial risk

2.3 Ambiguous valuation in balance sheet

Valuation of Bitcoin has not been very clear in the past. Crypto assets have the traits of commodities, currencies, and intangible assets. Because Bitcoin is not issued by a central bank, as is the case with feat currencies, it is more difficult to justify that it should be treated as a currency. This section explores some literature and accounting standards from the past which ponder on this issue.

A study conducted in 2015 by Dyhrberg concluded, that bitcoin is somewhere between a currency and a commodity because of its decentralized structure and limited market size at the time of the study. The study further revealed that, Bitcoin can combine the benefits that commodities and currencies hold in the markets and therefore can be used as a handy tool for management of portfolio, risk analysis and market sentiment analysis. (Dyhrberg 2016, 92.)

Commercial organizations around the world are starting to use cryptoassets for making payments and investments. It is important to not confuse the cryptoassets with feat currencies presented in digital form. Organizations that do transactions using cryptoassets have to encounter new kinds of accounting and tax requirements and new risks. Digital assets that can be classified as cryptoassets can vary from non-fungible tokens (NFTs) to digital art and cryptocurrencies like bitcoin. Most importantly, it is not a currency similar to feat currencies, because it is not issued by a central bank. (Mishler, 2021.)

Financial Accounting Standards Board (FASB) has done some investigation to figure out how cryptocurrencies should be valued. FASB concluded in its agenda consultation report that crypto assets can be classified under Topic 350, Intangibles – Goodwill and Other. This is because crypto assets match the description of intangible assets. (FASB 2021, 15.)

Invitation to comment (ITC) is issued when FASB needs consultation to develop GAAP.

In the FASB ITC meeting handout, it was mentioned that some companies have or are considering diversifying their investing strategy by including cryptocurrencies in their investments. Some companies are visualizing to accept payments in cryptocurrencies or use it as a method to pay their employees. Some companies are wary of investing in cryptocurrency because of its high volatility, lack of regulation and cyber risks. (FASB 2 2021, 9.)

Earlier in October 2020 the board came into conclusion that pre-agenda research and outreach indicated that the issues related to cryptocurrencies were not enough pervasive at the time. The research pointed out that companies either don´t have exposure to cryptocurrency-related issues, or they have but in very limited manner. According to the handout, there are companies that are very active in the crypto market. Those companies are functioning as investment companies, service providers (such as wallets) or as miners. (FASB 2 2021, 9.)

According to the American FASB Concepts Statement No. 5 transactions that for a transaction to be valid for presentation as a monetary measurement unit in the financial documents, it must be presented in currency form and have a stable value across time. Cryptoassets don´t meet these criteria. Therefore, transactions related to cryptoassets are treated with different accounting principles.

FASB has not added comprehensive standards on how cryptocurrencies should be valued and how the financial risk in them should be measured. Therefore, it is leaves more for the entity´s discretion to consider how the risks and valuation should be done. There are recommendations on how to do it, but no comprehensive standards.

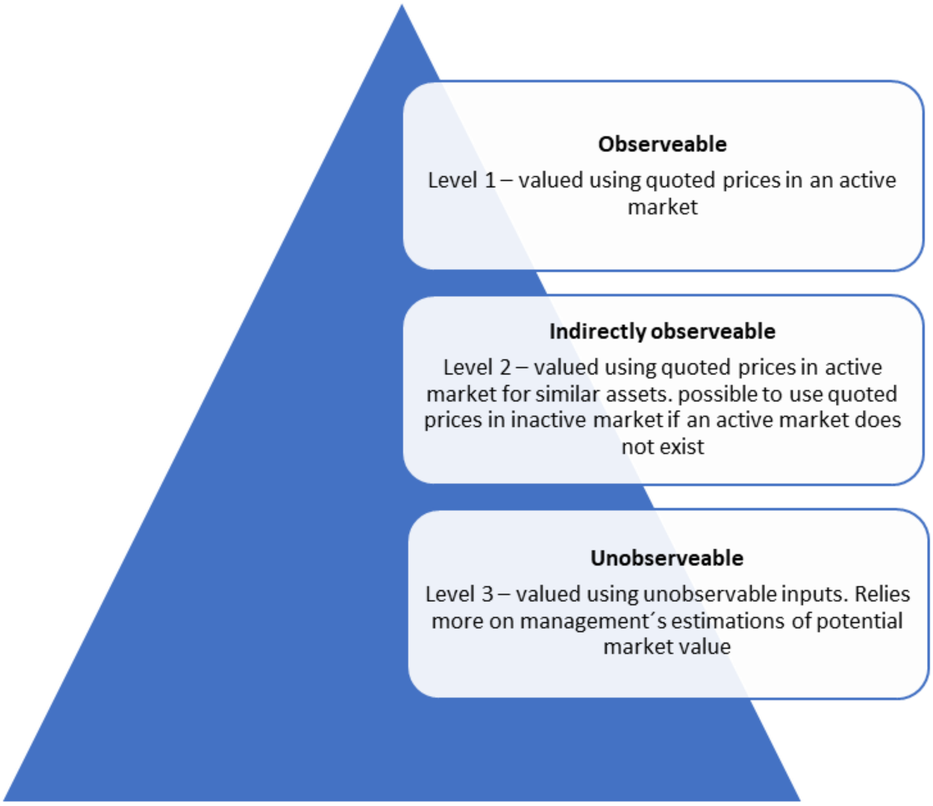

Figure 4. Fair Value Hierarchy

ASC820 standard provides some instructions how to value cryptocurrencies when they are measured on their fair values. The figure above demonstrates how the standard instructs to determine fair value of crypto assets.

ASC 820 – Fair value measurement by FASB categorizes inputs used in fair value measurement to three levels. Entities following ASC 820 are required to report quantitative and qualitative data used in fair value measurements. Level 1 and level 2 inputs rely on quoted prices in the active markets, and level 3 inputs are unobservable, and rely more on the management´s assumptions. (Deloitte 2021, 3.)

The fair value measurement framework and disclosure requirements are stated in the ASC 820, but the standard does not set requirements on when an entity is allowed to measure assets at fair value. These requirements missing from the ASC 820 are covered in other U.S. GAAP. (Deloitte 2021, 1.)

There is a consensus from the AICPA that cryptoassets should be categorized as intangible assets on the balance sheet. Their lifetime is also considered open-ended. FASB ASC Topic 350 defines an intangible asset with indefinite lifetime. If the intangible asset does not have normative, contractual, economy related or other factors that would determine the intangible asset´s lifetime, its lifetime can be considered indefinite. (Mishler, 2021.)

The indefinite assets are tested with something called “annual impairment testing”. As an example, if the asset´s value decreases and testing is conducted that comes into conclusion that there is an impairment, the commercial organization would acknowledge an impairment loss on the income statement. It is important to note that if the cryptoasset´s value restores or even goes beyond the previous highest value, the commercial organization is not allowed to consider it as a rise in value in the income statement. The commercial organizations should pay attention to impairment loss risk. Some impairment indicators can be the cryptoasset transactions the reporting organization makes itself, third-party market transactions that are cheaper in value compared to the value that reporting organization is carrying its cryptoassets with and other relevant events that may indicate impairment. (Mishler, 2021.)

Similarly, as FASB, the IFRS Committee sees in its agenda decision that holding cryptocurrency fits the IAS 38 definition of intangible asset. This is because it is a) capable of being separated from the holder and transferred individually: and b) it does not give the holder a right receive the currency in fixed or determinable numbers. (IFRS 2019, 1.)

The Committee´s interpretation of how cryptocurrency should be valued depends on how it is being used. IAS 2 Inventories applies for businesses that are holding them and planning to use them for sale in the regular business activity. If the purpose of use does not fit IAS 2, then IAS 38 should be applied when holding cryptocurrencies. The Committee also viewed the cryptocurrency as non-financial asset because it does not have the characteristics of cash or an equity. (IFRS 2019, 1-2.)

Additionally, if the entity is measuring holding of cryptocurrencies at fair value, IFRS 13 Fair Value Measurement lists disclosure requirements that should be followed. If there are material non-adjusting events, IAS 10 Events after the Reporting period needs to be followed. It obligates the entity to disclose information on the nature of the event and estimate its financial effect. If an estimate is not possible to be made, then statement needs to be done. For instance, if the cryptocurrencies changed in value drastically after the reporting period, it could influence economic decisions made by those using the financial statement. That is why disclosure would be relevant in such a situation. (IFRS 2019, 3.)

IAS 1 mentions that intangible assets should be reported as a line item in the statement of the financial position. (IAS 1, 1997) Change in the value of cryptocurrencies is determined with

IFRS 13 Fair Value Measurement, which is used for possible revaluation. The measurement in IFRS 13 is market-based. (IFRS 13, 2011) It is suitable to use it for measuring change in the value of cryptocurrencies because a market can be argued to exist when they are traded.

According to Finnish Accounting Standards (FAS), accounting entity must record its income, financial events, expenses and any other corrections or transfers as transactions. (Finnish Accounting Act 1997/1336) This is the reason why cryptocurrencies must be recorded in the financial statements in Finland.

In Finland, there are no cryptocurrency specific instructions on how to value them on the balance sheet. Instead, discretion is used, and the accounting act is followed where applicable. How cryptocurrencies are valued depends on what is their context of use. I think that valuation of cryptocurrencies is unclear in Finland.

	B Current Assets
	I Stocks
	1. Raw materials and consumables
	2. Work in progress
	3. Finished products/Goods for sale
KILA 1895/3.12	4. Other stocks
	5. Advance payments
	II Debtors
	1. Trade debtors
	2. Amounts owed by group undertakings
	3. Amounts owed by participating interest undertakings
	4. Loans receivable
	5. Other debtors
	6. Subscribed capital unpaid
	7. Prepayments and accrued income
	III Investments
	1. Holdings in group undertakings
	2. Other shares and similar rights of ownership
KILA 1895/3.7	3. Other investments
	IV Cash at bank and in hand

Figure 5. Finnish accounting board´s interpterion on how cryptocurrency should be presented on the balance sheet.

The Accounting Board (in Finnish: Kirjanpitolautakunta) has given a statement on cryptocurrency´s valuation and presentation on the balance sheet from accounting´s point of view. In a decision number 1895, the Accounting Board concluded that cryptocurrencies should be presented as “other stocks” or “other investments” in the balance sheet. If the organization is using cryptocurrencies for liquidity purposes, then “other investments” should be used. If they are used as part of regular business activities where they are sold, acquitted, and bought, they should be classified as “other stocks”. (KILA 1895, 2012.)

In addition, the accounting board stated that the accounting entity should explain in notes how the alternative currencies were valued so that the correct and adequate view required by accounting act can be assured. Further, the accounting board instructed that it is reasonable to create an explanatory note mentioning the total amount of alternative currencies when such information is relevant. If the cryptocurrencies are presented as “other stocks” under “stocks” and their value decrease below the acquisition cost, a write-down should be written according to Accounting Act. (KILA 1895, 2012.)

As of 2021	IFRS	FASB	FAS
Balance sheet regulation	IAS 2 Inventories & IAS 38 Intangible assets	Topic 350, Intangibles – Goodwill and Other	Accounting Act 1997/1336 & KILA 1895
Cryptocurrency definition	Non-financial, intangible asset, commodity	Intangible asset	Stock or investment
Cryptocurrency valuation	IAS 36 Impairment of assets	ASC 820 – Fair value measurement	N/A - No consensus

Table 3. Valuation and risk reporting according to international and Finnish accounting standards.

The table above conceptualizes which IFRS and FASB standards are meant to be followed when presenting cryptocurrencies on the balance sheet and how they should be valued. FAS, which stands for Finnish Accounting Standards is in the table for comparison. International accounting organizations and Finnish government who issued the standards that are in the table have mentioned an interpretation of whether the cryptocurrencies should be considered to be financial assets or other type of assets.

An IMF paper from 2018 instructs on treatment of cryptocurrencies when using them for macroeconomical statistics. It drew a distinction between those digital tokens issued by a central bank and those issued in the way similarly to how Bitcoin was issued. According to the paper, it does not matter is the digital token issued by a central bank based on DLT or not, it would be treated as a currency regardless of it. Similarly, digital currencies issued by institutional organizations are also treated as financial assets, even if they are using DLT. (IMF 2018, 7.)

The paper classifies digital tokens in to four types. Payment tokens, utility tokens, asset tokens and hybrid tokens. Payment tokens are described to work similarly to Litecoin, they are intended to be used as means of payment, to hold value or for measurement of units. Utility token on the other hand is meant to provide its holders access to some service that is based on DLT. Services like that could be for instance file storage or social messaging. Filecoin is an example of a utility token. Asset tokens represent debt or equity claims on the issuer. They are also capable of generating interest to its holder. It could also be used to provide its holder a promise to share earnings of the company in the future. Hybrid tokens are a mixture of utility token and asset token, or utility token and payment token. BLCA, described by IMF as “Bitcoin-like crypto asset”, should not be considered financial assets by the IMF´s instruction. These crypto assets are not issued by central banks or institutional organizations. (IMF 2018, 3, 7.)

At the time of publishment of the paper, the international accounting community suggested that BLCAs should not be treated as financial assets. There was no general decision on what kind of specific nonfinancial asset class should BLCAs be classified. The accounting treatment of crypto assets was under consideration by IASB. (IMF 2018, 9.)

3. RESEARCH METHODS

The research will be done mostly with hypothetic-deductive method, by presenting hypotheses that are based on the empirical literature and documents in the theoretical framework, and then observing whether the hypotheses are true or false by comparing them to newer research literature and financial statements. The research will include case studies, which use an inductive approach based directly on the annual reports.

3.1 Research question

This paper investigates what is the financial risk when an organization takes cryptocurrencies as part of their regular operation. It also examines how the cryptocurrency should be valued in the balance sheet if it is taken in use. Both its valuation and financial risk of using it are related to each other and its high volatility has significant effect on the financial risk it can pose. Therefore, it is necessary to review how it is represented on the balance sheet, and how it affects the profit.

Partially the issue of using cryptocurrencies in public activity of many governments, including the Finnish government, is related to the general unwillingness to use them for anything else than temporary confiscation related to law enforcement. The point of the study is not to focus on the law enforcement and money laundering perspective of cryptocurrencies. Instead, the study focuses on the financial risk when holding cryptocurrencies, investing in them, and using them for payments. Research is directed to be useful for hybrid, private sector and public sector organizations which engage in such and attempts to examine what degree of a financial risk a public sector organization in specific could face.

The study generates in-depth, non-numerical data and therefore will be qualitative as of its nature.

Baseline in qualitative research is describing real world phenomena. This is linked with an idea that the reality is diverse. Research should consider that it is not possible to divide the reality arbitrarily into parts. The phenomena shape one another, and it is therefore possible to find connections that span to multiple directions. The goal in a qualitative study is to investigate the target of research comprehensively. (Hirsjärvi et al. 2007, 157.)

The researcher can´t detach from values because values alter how we try to understand the phenomenon we attempt to study. It is not possible to achieve objectivity either in its traditional sense, because the researcher and what is known are intertwined. We can get as results only conditional explanations that are limited to a specific time and place. It is generally acknowledged, that in qualitative research the aim is to find or reveal facts than verify already existing facts that claim to be true. (Hirsjärvi et al. 2007, 157.)

The plan is to conduct a normative study that is supplemented by a systematic literature review, where different accounting standards are analysed to find out the requirements set on the presentation of cryptocurrencies on the balance sheet. It would also be crucial to examine what do the standards require of presentation of cryptocurrency-related risks. Alternatively, lack of requirements on the cryptocurrency risks and presentation will also be the focus of the study if there are little or no requirements mentioned.

The systematic literature view will give an updated academic perspective on the current risks that are emergent with cryptocurrencies. This literature review will both open a horizon to financial risk of cryptocurrency and reveal if the risks have changed over the time. Any new risks that did not appear in the theoretical framework should be found from the systematic literature review, any old risks that do not exist anymore, should be missing from the literature review.

Different cases of balance sheet presentations are reviewed to check how they valuate cryptocurrencies on their balance sheets and how they perceive the risks in holding, using, or investing in cryptocurrencies. The point would be to check what kind of risks are mentioned in the balance sheets and how. Finally, if there are requirements and standards set on cryptocurrencies and the organizations don´t follow them, that would also be the subject of this study.

Cryptocurrencies are a trendy, new phenomenon in the financial world and not much research has been done to investigate risks of using them and the potential benefits from the perspective of public sector organizations. There have been many private sector organizations who have used cryptocurrencies in their financial activity, but not many public sector organizations. Learning from the events that happened in these private sector organizations can provide valuable insight for what could hypothetically happen in public sector organizations.

Market direction of Bitcoin usually heavily correlates with most cryptocurrencies, but not all of them. Therefore, Bitcoin is generally a good cryptocurrency to focus on to understand the overall market. Low market cap can be swung more heavily by institutional investors and market conditions, making permanent loss of funds more likely. However, over time increasing market cap that is large, Bitcoin as a prime example, poses lower degree of risk.

The research will have the following main research question:

Are the cryptocurrencies as risky as before and are they valued in the balance sheet similarly to commodities?

It will also have the following three hypotheses which are used to answer the question:

1) Benefits of using cryptocurrencies have increased because financial risk of using cryptocurrency has decreased.
2) Cryptocurrencies are still speculative and risky assets at the time of making this study, but risks associated with them have decreased over time and likely continue to decrease
3) Cryptocurrencies are valued in the balance sheet similarly to commodities.

Systematic review is used to answer the first and second hypothesis, and case studies will answer the third hypotheses.

3.2 Systematic literature review

In this study I will be assessing total financial risk cryptocurrency can pose for an organization using it. To obtain an understanding of the total financial risk, I will be breaking down financial risk in to its four sub-risks mentioned by Christoffersen and check whether the risk-level of these sub-risks has increased or not. I will explain more in detail how will I measure the risk-level of these sub-risks in financial risk.

I will analyse every market risk, liquidity risk, operational risk and credit risk using a systematic literature review. The point is to find out the changes in the risks and find out whether using cryptocurrency has become less risky.

I will delimit the literature review to years of 2018, 2019, 2020 and 2021. As mentioned, there will be a 4-year period that is set after the empirical literature. The empirical literature in the theoretical framework is from the years of 2013-2017. The latest literature from 2018 onwards will be compared with the literature dating 2017 and before. This way the intersection of the literature in the theoretical framework and the literature review is set on the same time when cryptocurrency bubble burst in 2018. The risks from both the theoretical framework and the material will be compared to find anomalies on whether the ratio between risks have changed and to which direction.

Systematic literature review is used rather than, for example, descriptive review, because findings between the recent and previous research literature will be mirrored to one another. Scientific literature that was used in theoretical framework but not in the systematic literature review is important for the research it helps to conceptualize the crypto economy, which is relatively new and still constantly evolving phenomenon in the financial world. The literature review will use general cryptocurrency risk literature and bitcoin security literature.

3.2.1 Search strategy

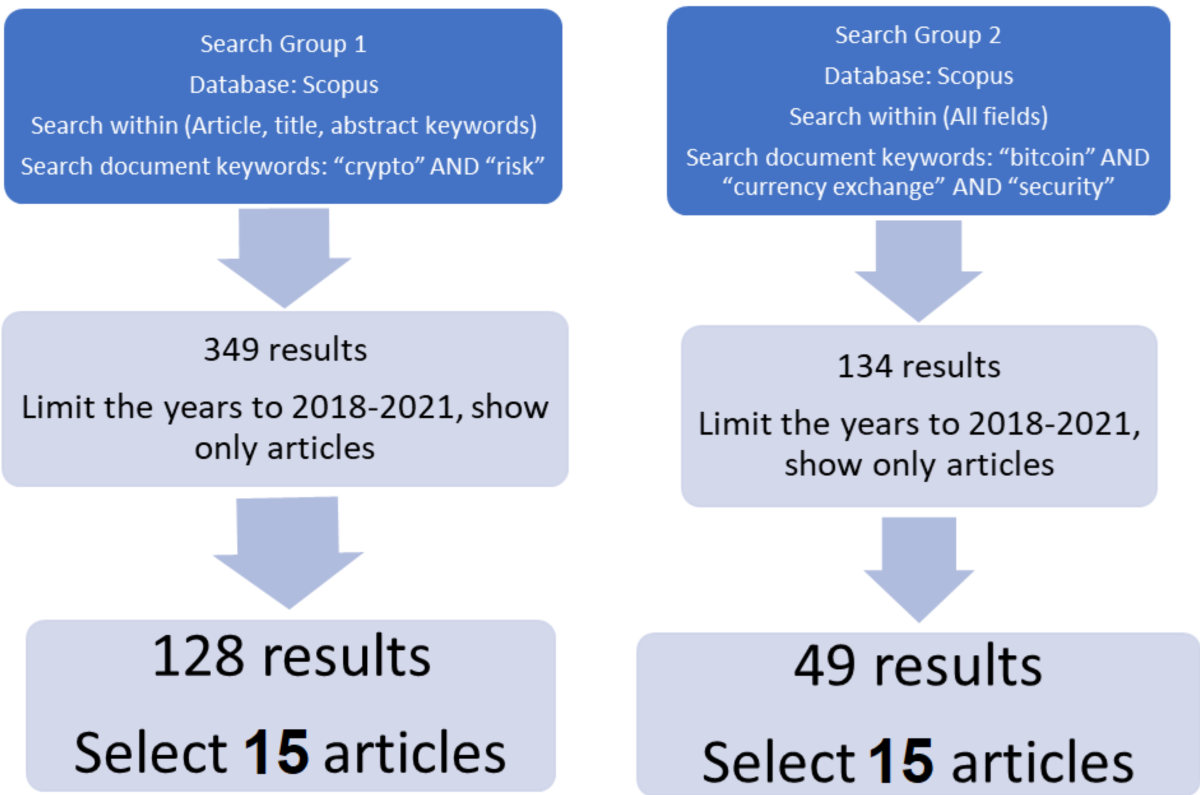

Figure 6. Search strategy

I will use databases Scopus, ScienceDirect and Web of Science to find research literature dated 2018 and after. Scopus will be used primarily, and other databases are used to supplement searches where Scopus is lacking. Only English literature will be selected, and most highly cited articles favored. The systematic literature review consists of two distinct searches where different keywords are used.

The first search will be inputted to Scopus in the following way: “crypto” AND “risk”. A field filter is added to search inside “Article title, Abstract, Keywords”. This leads to 349 results, which are further reduced by limiting the years to 2018-2021 and filtering out all document types except articles. After setting the new filters and searching again, it will lead to 128 results. The articles will be selected based on their relevancy to this study and highly cited articles are favored when possible. Out of these 128 results 15 articles are selected.

The second search will be inputted to Scopus with a different field filter. The filter will include all “All fields”. The following keywords are used: “bitcoin” AND “currency exchange” AND “security”. It leads to 134 results. The years are limited to 2018-2021 again and only articles are selected. The search is re-done, and the search will give 49 results. The selection happens with the same relevancy and citation-favoring criteria as in the first search. 15 articles will be selected, which leads in total of 30 articles selected.

The next database searched is ScienceDirect. The fields “title, abstract or author specified words” is selected. Keywords “crypto” AND “risk” are used. It gives 44 results. 2 articles are selected.

There third database searched is Web of Science with all fields and keywords “crypto” AND “risk” it gives 187 results. When searched is limited to years from 2018 to 2021 and only articles included, the search is done again, and it gives 88 results. 3 articles are selected.

№	Article	Authors	Published	Journal	Search Group
N1	Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems	Renwick, R. & Gleasure, R.	2021	Journal of Information Technology	1
N2	The predictive capacity of GARCH-type models in measuring the volatility of crypto and world	Naimy V, Haddad O, Ferna´ndez-Avile´s G, El Khoury R	2021	PLoS ONE	1

	currencies				
N3	Bitcoin and altcoins price dependency: Resilience and portfolio allocation in covid-19 outbreak	Aysan, A.F., Khan, A.U.I., Topuz, H	2021	Risks 9	1
N4	Modeling the optimal diversification opportunities: the case of crypto portfolios and equity portfolios	Aliu, F., Nuhiu, A., Krasniqi, B.A. & Jusufi, G	2021	Studies in Economics and Finance, 38	1
N5	Tail risk measurement in crypto-asset markets	Ahelegbey, D.F., Giudici, P., Mojtahedi, F.	2021	International Review of Financial Analysis, 73	1
N6	A multivariate approach for the simultaneous modelling of market risk and credit risk for cryptocurrencies	Fantazzini, D. & Zimin, S.	2020	Journal of Industrial and Business Economics	1
N7	Does Bitcoin behave as a currency?: A standard monetary model approach.	Hui, C.-H., Lo, C.-F., Chau, P.-H. & Wong, A.	2020	International Review of Financial Analysis, 70	1
N8	Dynamic linkages among cryptocurrencies, exchange rates and global equity markets	Kostika, E., Laopodis, N.T.	2020	Studies in Economics and Finance, 37	1
N9	Investing with Cryptocurrencies - A Liquidity Constrained Investment Approach	Trimborn, S., Li, M. & Härdle, W.K.	2020	Journal of Financial Econometrics, 18	1
N10	Challenges when auditing cryptocurrencies	Vincent, N.E. & Wilkins, A.M.	2020	Current Issues in Auditing, 14	1
N11	On the nature and financial performance of bitcoin	Alfieri, E., Burlacu, R. & Enjolras, G.	2019	Journal of Risk Finance, 20	1
N12	Regulation of Crypto Tokens and Initial Coin Offerings in the EU: De lege lata and de lege ferenda	Burilov, V.	2019	European Journal of Comparative Law and Governance,	1
N13	What's left after the hype? An empirical approach comparing the distributional properties of traditional and virtual currency exchange rates	Hempfing, A.	2019	PLoS ONE, 14	1
N14	Bitcoin, crypto-coins, and global anti-money laundering governance	Campbell-Verduyn	2018	Crime, Law and Social Change, 69	1

N15	A survey on security and privacy issues of bitcoin	Conti, M., Sandeep, K.E., Lal, C., Ruj, S.	2018	IEEE Communications Surveys and Tutorials, 20	1
№	Article	Authors	Published	Journal	Search Group
N16	2021 Knowledge Discovery in Cryptocurrency Transactions: A Survey	Liu, X.F., Jiang, X.-J., Liu, S.-H. & Tse, C.K.	2021	IEEE Access, 9	2
N17	Time series analysis of Cryptocurrency returns and volatilities	Malladi, R.K., & Dheeriya, P.L.	2021	Journal of Economics and Finance, 45	2
N18	Risk spillover between Bitcoin and conventional financial markets: An expectile-based approach	Zhang, Y.-J., Bouri, E., Gupta, R., Ma, S.-J.	2021	North American Journal of Economics and Finance, 55	2
N19	Exploring the driving forces of the Bitcoin currency exchange rate dynamics: an EGARCH approach	Zhou, S.	2021	Empirical Economics, 60	2
N20	Does Bitcoin behave as a currency?: A standard monetary model approach	Hui, C.-H., Lo, C.-F., Chau, P.-H. & Wong, A.	2020	Financial Analysis, 70	2
N21	Challenges when auditing cryptocurrencies	Vincent, N.E. & Wilkins, A.M.	2020	Current Issues in Auditing, 14	2
N22	Characterizing cryptocurrency exchange scams	Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X. & Xu, G.	2020	Computers and Security, 98	2
N23	A survey on blockchain cybersecurity vulnerabilities and possible countermeasures	Hasanova, H., Baek, U.-J., Shin, M.-G., Cho, K. & Kim, M.-S.	2019	International Journal of Network Management, 29	2
N24	“The most trustworthy coin”: How ideology builds and maintains trust in bitcoin	Knittel, M., Pitts, S. & Wash, R.	2019	Proceedings of the ACM on Human-Computer Interaction,	2
N25	Can artificial intelligence enhance the Bitcoin bonanza	Silva de Souza, M.J., Almudhaf, F.W., Henrique, B.M., Silveira Negredo, A.B., Franco Ramos, D.G., Sobreiro, V.A. & Kimura, H.	2019	Journal of Finance and Data Science, 5	2

N26	Bitcoin and cybersecurity: Temporal dissection of blockchain data to unveil changes in entity behavioral patterns	Zola, F., Bruse, J.L., Eguimendia, M., Galar, M. & Urrutia, R.O.	2019	Applied Sciences (Switzerland), 9	2
N27	The virtual currency regulatory framework in global context	Brown-Hruska, S. & Wagener, T.	2018	Capital Markets Law Journal, 13	2
N28	A survey on security and privacy issues of bitcoin	Conti, M., Sandeep, K.E., Lal, C. & Ruj, S.	2018	IEEE Communications Surveys and Tutorials, 20	2
N29	Price manipulation in the Bitcoin ecosystem	Gandal, N., Hamrick, J.T., Moore, T., Oberman, T	2018	Journal of Monetary Economics, 95	2
N30	Revisiting the risks of bitcoin currency exchange closure	Moore, T., Christin, N. & Szurdi, J.	2018	ACM Transactions on Internet Technology,	2

Table 4. Selected Scopus articles for systematic literature review.

The selected articles from the Scopus are listed in the table above. There is not much research done on the risks of cryptocurrencies from an organizational point of view, so the searches were not restricted to include specific journals only. The articles were selected from multitude of journals to get enough literature to cover the needs of this systematic literature review. Rest of the articles from ScienceDirect and Web of Science are listed in the table below. Overlapping articles were eliminated.

Secondary searches					
№	Article	Authors	Published	Journal	Database
N31	On cryptocurrencies as an independent asset class: Long-horizon and COVID-19 pandemic era decoupling from global sentiments	Sifat, I.	2021	Finance Research Letters Vol 46.	ScienceDirect
N32	A great disturbance in the crypto: Understanding cryptocurrency returns under attacks	Ramos, S., Pianese, F., Leach, T. & Oliveras, E.	2021	Blockchain: Research and Applications	ScienceDirect
N33	Dance with the devil? The nexus of fourth industrial revolution, technological financial products and volatility spillovers in global financial system	Umar, M., Rizvi, SKA. (Rizvi, Syed Kumail Abbas) & Naqvi, B.	2021	Technological forecasting and social change	Web of Science

N34	Critical slowing down associated with critical transition and risk of collapse in crypto-currency	Tu C, D'Odorico P. & Suweis S.	2020	Royal Society Open Science, 7	Web of Science
N35	Conditional tail-risk in cryptocurrency markets	Borri, N.	2019	Journal of Empirical Finance	Web of Science

Table 5. Selected articles from ScienceDirect and Web of Science.

3.3 Case studies

There will be normative case studies to find any hints of the future direction of accounting when it comes to valuation of crypto assets in balance sheet. Validity of this normative study is ensured by picking material from official accounting standards such as FASB and IFRS which issue accounting standards and using Finnish accounting standards for later comparison.

I will compare the FASB and IFRS standards mentioned in the theoretical framework with annual reports of different organizations to check how the cryptocurrency is valued on the balance sheet and if the standards are followed when it is presented on the balance sheet. This comparison would answer the question, whether the cryptocurrencies are valued in the balance sheet like commodities. I will also try to find how are the risks presented that emerged from the systematic literature review.

The case study is done as an explanatory case study, where the goal is to find causal relation between the international accounting standards and the way the cryptocurrencies are presented in the balance sheet. By finding out how the companies present cryptocurrency in their balance sheets, it is possible to know the current state of how accounting of cryptocurrencies is done in different companies and understand what to extent the existing norms and recommendations set by the international accounting standards are followed. Additionally, the goal of the case studies is to find out if and how the companies explain their cryptocurrency related accounting decisions.

Even though examining one or multiple cases won´t achieve the purpose of obtaining universally applicable data, I argue it to be one of the most effective ways to research the complicated and ambiguous concepts of financial risk in cryptocurrencies and the accounting of cryptocurrencies. The systematic literature review on financial risk can be used to help explain some of the risk related concerns the companies report on their balance sheets.

In Finland, cryptocurrencies are used in very limited manner in government agencies. Usually, cryptocurrencies are obtained through law enforcement activity, but they are not actively being used otherwise. For this study I will present a case of accounting from Finnish Customs, which brings a different reporting point of view to the study.

Finnish accounting standards will be used mainly for the Finnish Customs case study and for later comparison of international standards. The perspective that this research aims at, is a European perspective and an international perspective. Balance sheets from two American and two European companies are included as cases in the study to bring more American and European accounting perspective. The study intends to examine how the cryptocurrency is valued according to international standards and European norms.

3.3.1 Case material - Documents

The material for the case studies is taken from annual reports found on the web. These reports provide comprehensive view of the risks the case organizations face when using cryptocurrencies. The reports also explain how the cryptocurrency is valued and which international standards are followed. Because the reports give all the information required in this study, the cases are focused only on the annual reports.

Organization	Document Name	Organization type - sector	Pages
MicroStrategy Inc	2020 Annual Report	Company - Private	112
Tesla Inc	Form 10-Q	Company - Private	60
Finnish Customs	Tullin tilinpäätös vuodelta 2020	Agency - Public	57
Bitcoin Group SE	Annual Report 2020	Company - Private	107
Argo Blockchain	Annual Report Accounts	Company - Private	61

Table 5. Organizations examined in the case studies

4. MATERIAL ANALYSIS

4.1 Summarization of data from literature

4.1.1 Market risks

Naimy et al. (2021) conducted a study where they compared volatility of bitcoin and 5 other major cryptocurrencies with volatility of feat currencies. In the study they analyzed the capacity of different GARCH-type models to measure the volatility of cryptocurrencies and feat currencies. They chose to run tests on the cryptocurrencies from a period of October 13th, 2015, till November 18th, 2019, using seven of these GARCH-type models mentioned earlier. (Naimy et al. 2021, 3-4.)

Similarly, to how Dyhrberg discovered that bitcoin is sensitive to shocks, the study found that bitcoin´s volatility is sensitive to positive and negative shocks. (Naimy et al. 2021, 11). The study evidenced that bitcoin has periods where it is more highly volatile and emphasized that these periods can be persistent. This matches with Dyhrberg´s findings related to bitcoin´s changing periods of relative stability and higher volatility.

My view is, that because the study had the most well-established cryptocurrency bitcoin as the target of study, it gives a good indication of the crypto market´s volatility over four-year period till 2019. Their research came into the conclusion that the most stable cryptocurrency of those studied in the research is 10 times more volatile than feat currencies. They further argued that the cryptocurrencies don´t fit to be alternatives for feat currencies and recommended the authorities to regulate the cryptocurrencies further. Because of all this, the researchers advised investors to not invest excessively into cryptocurrencies (Naimy et al. 2021, 14-15.)

In addition to volatility, the market risk is affected by systematic risk that comes from macroeconomic and political factors. Smart contracts and networks can steer the market, which can lead to some challenges. Paech mentioned that there can either be one large network, or multiple different networks handling the transactions.

Aliu´s study argues that cryptocurrencies don´t pose systemic risk because their global market size is not large enough. (Aliu et al. 2021, 52). If Paech´s prospections about systemic risk and systematic risk are taken into consideration, it seems that these risks are possibly more relevant in the future. Once the crypto market matures and gains a solid market size, it could be likely that either one of these two risks are going to elevate the possible market risk. Ahelegbey et al. (2021) describes systemic risk broadly: "systemic risk can be thought of as a widespread failure of financial institutions or as a freezing up of capital markets which can substantially reduce the supply of such critical intermediation". Further, Ahelegbey argues that return volatilities are caused by systemic risk, systematic risk, and tail risk. (Ahelegbey et al. 2021 1.)

Knittel, Pitts & Wash (2019) defined the biggest systemic risk as acceptance of invalid transactions in the Bitcoin´s system. Invalid transaction makes the double spending problem possible, and the consensus algorithm is the only protection against this problem. The participants must follow the algorithm correctly for it to work as intended. (Knittel, Pitts & Wash 2019, 5-6.) Depending on the point of view taken in a study, the concept of systemic risk can be understood in different ways. The common ground seems to be, that systemic risk can be thought of as a failure of a system handling the transactions. These systems can be financial institutions or decentralized blockchains.

Aliu´s mentioning of cryptocurrencies not correlating with stocks can provide an opportunity for portfolio diversification, which makes the portfolio less susceptible for risks in the stock market. (Aliu et al. 2021, 52). Alfieri et al. considers cryptocurrencies as having potential for diversification due to its low correlation with other asset classes. (Alfieri 2019, 118). Umar et al. conducted a study volatility spill overs in global financial system, and this study confirms the low correlation of cryptocurrencies with other asset classes, as was found in Aliferi´s study. (Umar et al. 2021, 8). Zhang Y.-J. et al. (2021) found that the Bitcoin risk could change the risk of conventional assets, which makes it a relevant phenomenon for policymakers and regulators. (Y.-J. et al. 2021, 9). In addition, Malladi & Dheeriya discovered smaller cryptocurrencies such as XRP being more sensitive to traditional assets and having causal effect on bitcoin prices. (Malladi & Dheeriya 2021, 92). Bitcoin itself is isolated from the world economy and its correlation with the world economy is correspondingly low. (Zhou 2021, 600).

Cryptocurrencies are highly correlated and provide less diversification opportunities for investors. Other coins tend to be influenced by price movements of bitcoin and Ethereum. High interdependency of cryptocurrencies limits the diversification possibilities of investors who build their portfolio solely out of cryptocurrencies. Moreover, previous studies have indicated that investors who are investing to multiple different assets in addition to cryptocurrencies gain the benefit of reduced diversification risk (Aliu et al. 2021 52, 60.) When cryptocurrencies are used as investments, interdependency risk should be paid attention to. Interdependency of cryptocurrencies should encourage investors to diversify and not solely invest all the portfolio into cryptocurrencies. Borri´s study on conditional tail-risks in cryptocurrencies confirms that cryptocurrencies are highly correlated with one another and poorly correlated with other global assets such as gold. (Borri 2019, 14.)

Rising variability in the cryptocurrency prices can be taken as a warning signal of systemic risk. This takes in account the existing analogy between the cryptocurrency markets and complex ecological systems. Tu, D'Odorico & Suweis investigated cryptocurrencies and the susceptibility of their daily closing prices to critical transitions. They aimed to estimate the risk of collapse in complex system when underlying dynamics are unknown. They focused on cryptocurrencies that covered more than 85% of the cryptocurrency market capitalization and analysed different cryptocurrencies from the time period of 1st January 2016 to 31st March 2018. (Tu et al. 2020, 2.)

When the complex system has underlying dynamics that are not known, early warning signatures still exist, and major indicators can be used to detect the critical points before it transitions to critical state. (Tu et al. 2020, 8). This finding could be used to handle the problem mentioned by Paech where several networks cause a complex systematic risk. Tu, D'Odorico & Suweis analysed multiple cryptocurrencies spanning several networks.

Even though cryptocurrencies use several networks when they are viewed as a group, their price developments are interdependent. This interdependency can be presented as a risk but also as a possibility to understand the complexity of the networks. However, not all cryptocurrencies are interdependent. There are "stable coins" such as tether, which have the same price and unchanged price development. Second good example would be "hype coins", which have a price development more driven by media coverage and social media popularity rather than regular market activity. A study by Kostika E. & Laopodis N. T. indicated that cryptocurrencies were susceptible to market events and attacks of speculative nature. They can offer a decent short-term investment when the portfolio is diversified to global assets. (Kostika & Laopodis 2020, 263.)

It could be argued that when Aliu mentioned that building an investment portfolio out of cryptocurrencies is risky due to high interdependence, it would be not as risky if the portfolio included cryptocurrencies that were exceptionally interdependent. That could significantly reduce complexity risk. It would still be subject to factors related to volatility risk presented by Dyhrberg, but most other causes exposing cryptocurrencies to market risk would play significantly lesser role when assessing riskiness of the portfolio.

When it comes to volatility with cryptocurrencies, a crash risk is always present. Hui et al. (2020) discusses that the bitcoin´s exchange rate shares some similarities with commodities that have crash risk. Crash risk can be described as a burst of bubble, as was seen in 2018. (Hui et al. 2020, 1.) In addition to volatility, there seems to be a cyclical element to the market. Existence of this cyclical risk is acknowledged by Aysan et al., who state in their article that cryptocurrencies are affected by cyclical risks and volatility in the global financial system. (Aysan et al. 2021, 11.)

4.1.2 Liquidity risks

According to Kirillova et al. (2018) a legal framework on cryptocurrencies would solve various problems. It would provide a legal protection on market participants, create bridgehead for taxation and combat fraud. (Kirillova et al. 2018, 124.) When cryptocurrencies are used online, a big part of the liquidity risk is the lack of regulation on payments and activities surrounding them. There are participants who try to exploit the lack of legal framework by committing various kinds of frauds and many service providers hosting or developing cryptocurrency related services have also exploited the unawareness of the regular cryptocurrency user and the lack of legal framework.

As Luther mentioned, absence of regulation can create a legal grey area. This makes the whole crypto space a risky avenue for those that expect stability and security. Kirillova stated that a legal framework would provide this legal protection. (Kirillova et al. 2018, 124.) It was estimated in the Kirillova´s study that the bitcoin would become relevant in the world´s economy as its market capitalization would hit 100 billion dollars and the cryptocurrency exchanges are obliged to follow anti-money laundering directive. (Kirillova et al. 2018, 124).

The fifth anti-money laundering directive (5AMLD) came in effect in 2018, which means that regulation has increased in the time frame between Kirillova´s and Luther´s studies.

Lack of regulation is still a relevant risk. Legal status of the virtual currency depends on legislation of different countries. The countries have different legislation on cryptocurrencies, and they vary significantly. Crypto currency is most often referred to as electronic money, surrogate of money, stock exchange asset or virtual currency. (Kirillova et al. 2018, 120.) My view as the writer of this paper is that while some countries could end up banning cryptocurrency, which Luther mentioned as a risk, called as "conflict with state control" in the theoretical framework, many countries seem to see it as a supplement to the existing monetary system. This can be concluded from the type of legislation that has been prepared for example in the U.S and Europe. China has ended up banning cryptocurrencies (as of September 2021).

Kirillova asserted that the main problem with cryptocurrency is the definition of its legal essence. Is the cryptocurrency a new kind of electronic money or a temporary economic phenomenon that has no future to exist as a significant part of monetary system later? If the crypto currency will become and is considered as electronic money, then the circulation of it should get a legal support. (Kirillova et al. 2018, 121.) This problem is in line with the problem Luther defined, where many accept the underlying blockchain technology that bitcoin is based on, but many doubt the bitcoin itself.

Renwick, R., and Gleasure R. noted in their article how designing regulation can be challenging when the technology is relatively new. This is the case with blockchain technology. Scale of risks are usually unclear, and the governments do not want to halt the innovation by implementing regulation prematurely. (Renwick & Gleasure 2021, 18.)

On the other hand, Brown-Hruska & Wagener mention on their article that many international regulatory frameworks meant for cryptocurrencies are incompatible and inconsistent, giving the market more potential for fragmentation. (Brown-Hruska & Wagener 2018, 492). Other researchers conclude similarly as well, such as Hempfing A. (2019) who states that bitcoin and other crypto coins are subject to various regulatory risks, which raises consumer protection and financial crime related problems. (Hempfing 2019, 4).

Legal essence of the bitcoin can be better understood if the essence of non-cash money is specified. Some scientists believe the non-cash money have all the powers of the owner while a bank note is equivalent only to a certain amount of money. Property is determined by the sum of monetary units represented by a bank note, not bank notes themselves. (Kirillova et al. 2018, 121.)

Money that is in cash form is usually backed by the government. Government backed currency lets the government to enact monetary policy and confiscate the funds, as mentioned by Luther. Non-cash money that bitcoin and other cryptocurrencies present might conflict with these interests. My perspective is that cryptocurrencies need to have benefit for the governments to offset these interests. This issue is different in a western democratic government than for example in a less democratic, authoritative government. Therefore, I believe that the risk of conflict with state control is more major in a non-western, non-democratic government than in a western democratic government.

The concept of non-cash money is somewhat abstract and contains two elements. One is electronic money stored on virtual data carriers and the other is the mechanism for accessing an account through bank cards and non-cash transfers. When talking about cryptocurrencies, the users around globe are increasingly recognising the convenience and efficiency of virtual currencies.

In the United States, virtual currency is seen in three ways. It is seen as an analogue of money, property, and commodities. In the July 2017, the US Securities and Exchange Commission (SEC) submitted a Statement about initial coin offerings. SEC saw it necessary to subject initial coin offerings to legal regulation. This would let the cryptocurrency to become a recognized investment possibility. Office of the Comptroller of the currency is also planning to make state restricted banking license available when it comes to fiduciary activities related to cryptocurrencies. (Kirillova et al. 2018, 123.) The Securities and Exchange Commission listed lack of insurance protection for bitcoins as a risk. (Silva de Souza et al. 2019, 86).

The newer research literature between the years of 2018 to 2021 did not mention the liquidity risk related to money market funds allowing instant withdrawals for the customers. According to Lin, Whinston and Fan (2015) this was the problem the Chinese authorities were concerned about in 2014. Primarily, the fact that they could expose the market to quick changes in liquidity, cause liquidity problems for the funds and might make a chunk of the investor´s funds disappear were the main concerns expressed.

As seems apparent in the Kirillova´s study, the government agencies have been paying attention to the development of the cryptographic economy, and some governments around the world have taken measures to implement some regulation. Especially in Europe there is now clear regulation the exchanges and other intermediaries must follow the Europe´s 5AMLD. China on the other hand, has resorted to banning cryptocurrencies, which was not the case yet at the time Lin´s study was published.

The crypto market is bigger in 2021 when comparing its total market capitalization to that of the 2014. This means that the funds might not be able to affect the market that much anymore because it is bigger. In addition to that, the governments have either started to or are planning to regulate cryptocurrencies if they allow them, or outright ban them totally, as in China, or partially, as in Russia. There are now many cryptocurrency exchanges and funds that have existed for several years and gained a solid reputational and financial grounding. This could also make the risk related to instant withdrawal significantly less problematic as it was in the past.

Imtiaz Sifat conducted a study on cryptocurrency as an independent asset class. The study discovered the dissociation of crypto market events from global sentiment proxies ranging from 2015 to 2021. The findings became more potent on the COVID-19 period and figured out that there is increasing pressure for treating cryptocurrencies as an independent asset class. (Sifat 2021, 7.)

It seems overall clearer now where cryptocurrencies will be prohibited and where they will be allowed under regulation. It is still possible that some countries which have had a neutral stance on cryptocurrencies might ban it and at the same time ban any financial services offering cryptocurrency related services in the country.

4.4.3 Credit risks

A study conducted by Fantazzini which focused on modelling market risk and credit risk of cryptocurrencies, provided a new definition for the concept of "credit risk". The study defined credit risk so that it means the situation where the price of the cryptocurrency per unit drops tremendously, and the cryptocurrency becomes illiquid. Fantazzini describes that this would be the "death" of the crypto coin, adding that the crypto coin could still be revived from this state. The reason some dead coins still have some minor trading volume is because some either bet on the possible revamp of the coin or attempt to get a portion of their initial investment back. He further added that there is no clear definition of a dead coin in the research literature. (Fantazzini 2020, 20-21.)

Fantazzini revolves the whole concept of a credit risk in cryptocurrencies around the event of gains and losses where a cryptocurrency is abandoned and considered “dead”. This view is opposed to the definition of credit risk in traditional finance, where it is defined as the gains and losses on a portfolio associated with the failure to fulfil contractual obligations. The study measured credit risk related to the probability of a cryptocurrency dying. (Fantazzini 2020, 21.)

The price of the coin dropping so low that it could be considered a dead coin was because of the discovery of a scam, a hacker attack, or other reasons. (Fantazzini 2020, 30). Observing credit risk from this kind of viewpoint is unique to this study. For instance, Moore et al. 2018 investigated credit risk from the perspective of cryptocurrency exchanges closing. There seems to be no clear definition of credit risk in the context of cryptocurrencies.

The paper focused on estimating credit risk for small and medium-sized portfolios containing solely cryptocurrencies. It had an estimation of measures taken to handle credit risk for 42 coins, 13 of which were dead coins. (Fantazzini 2020, 35.)

An important finding in the study was that credit and market risks for cryptocurrencies were more interlinked than for traditional assets. Appearance of market risk and credit risk in the cryptocurrency market depends on if the coin is alive or dead. Market risk and credit risk both mean the gains and losses on the value of a portfolio of cryptocurrencies, but more specifically market risk manifests as gains or losses in alive cryptocurrencies and credit risk in gains and losses of dead cryptocurrencies. (Fantazzini 2020, 55.)

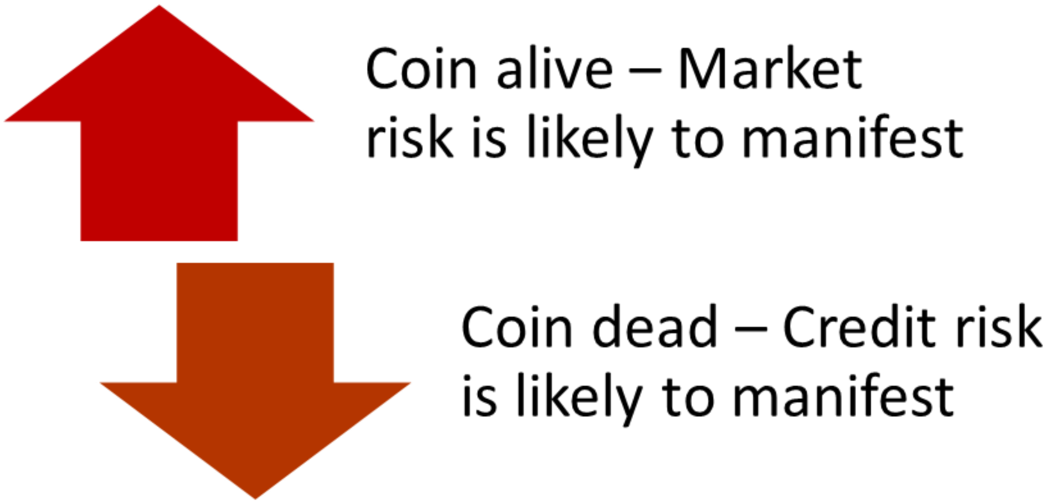

Figure 7. Coin vitality indicator

Earlier in 2013 Moore et al. published a study about credit risk from the context of cryptocurrency exchanges closing. They made a newer study in 2018 where they revisited these risks and checked if there is difference between the findings after the time of publishing the original study.

They made a new finding related to the security breaches. If an exchange experienced a security breach during a specific quarter, there was a correlation supporting it closing the same quarter. This finding did not exist in the original study. They explained that the finding was made possible due to longitudinal analysis that was possible to conduct because the observation of the phenomenon in the newer study was possible on a longer time scale. (Moore et al. 2018, 16.)

Secondary new finding they made was the correlation between competition and exchange´s continued operation. Exchanges that derived 90% of their activity from trading a currency that was traded at most by one competitor, were significantly less likely to close. The phenomenon of the exchange closure can be understood with regression, exchanges which faced low competition were 91% less likely to close. (Moore et al 2018, 16.)

How the closure affected the investors, was not elaborated in the research. The research did mention that some customers lost deposits when exchanges closed, but this was not investigated in detail. This is usually a dispute between the exchange operators and customers and there is no legislation addressing closure of an exchange directly. The paper also addressed the risk of investing in an exchange when its risk of closure is assessed. (Moore et al 2018, 16.)

The newer research defined exchange breach as an event, where the exchange users lose funds due to the negligent or incorrect conduct of the operators maintaining the exchange. The definition excludes phishing attacks targeted against the exchange users. There are different scenarios which can lead to the security breach. One of the common breaches happen when the breacher vulnerabilities in the exchange´s software, hardware, or configuration of the system to steal funds. (Moore et al 2018, 5.)

According to Moore´s figure data, probability of an exchange being breached peaked during the years of 2013 and 2014. Then the probability declined by more than 50% in the year of 2015. (Moore et al 2018, 11.)

One primary risk a crypto exchange can pose for the investors is that whether it will refund the lost funds if the exchange is closed. In the Moore´s study they were able to obtain 16 cases out of the total of 38 closed exchanges, where it is possible to know whether the customers were reimbursed or not. In six cases out of 16, they were not refunded. In the remaining 10 cases they were refunded either fully or partially. (Moore et al 2018, 7.)

4.4.4 Operational risks

Rahouti et al. described the decentralized governance and its weaknesses in their study. They described it as the first fully decentralized system where the monetary power is not controlled by anyone. They listed a few features that limit the system: the transactions are publicly saved; new bitcoins are generated by anyone and transactions on ledgers need to validated by a distributed network. (Rahouti 2018, 67191.)

Decentralization can bring governance issues, abuse of power, and change of protocols as Peters (2016) mentioned. In my opinion these have been traditional issues of the decentralized blockchain, which appear in many research papers. Peters explained that some problems stem from the way the blocks are validated. Theoretically, an attacker with enough CPU power to form a majority could fork the blockchain or make transaction blocks. Rahouti (2018) discusses these issues in detail.

Gandal et al. discussed price manipulation in their paper called “Price manipulation in the Bitcoin ecosystem”. Despite the increase in market capitalization, price manipulation remains a relevant problem especially for the coins that have smaller market capitalization. Their research indicated thin markets exhibiting sudden increases in trading volume that drive the exchange rate upwards. (Gandal et al. 2018, 96.)

To address the challenges related to the resilience of the decentralized Bitcoin, Rahouti´s article mentions that the system can be exploited in ways of fraud and hacking. (Rahouti 2018, 67196) Burilov´s article agrees with there being resilience challenges with Bitcoin, attributing it to the decentralized IT-structure. Burilov argues that the Bitcoin is vulnerable to hacking and can potentially cause a wide variety of operational risks. (Burilov 2019, 157.)

The article mentions further security threats that emanate from the decentralized nature of the Bitcoin. For instance, the Proof-of-Work based protocol is vulnerable to an attack where the attacker aims to gain 51% of the mining power. This would give the attacker a majority and possibility for the attacker to create any kind of transaction block. The attacker could also fork the blockchain. An attacker can make further attacks such as DoS and double spending. (Rahouti 2018, 67196.) Hasanova & Kim (2019) stated that while a blockchain might easily mitigate an attack directed against the entire network, a coded intrusion, such as a vulnerability in a single system can have wide negative consequences across the system. (Hasanova & Kim 2019, 27).

Bitcoin uses a peer-to-peer network to rapidly distribute data. It does so to achieve consensus faster. The article mentions some challenges associated with P2P-networks. The Bitcoin´s critical functionality is based on the consensus mechanism. To prevent a double spending vulnerability, the P2P-network must guarantee dependable scalability. There is a configurative process that helps reduce the netsplit risk. This is achieved when peering nodes choose their peers randomly and the list of peers is updated after a time interval. (Rahouti 2018, 67195.)

Peters (2016) listed both decentralized governance and P2P-networks as vulnerabilities. Even though they are both very closely related to each other, they still pose different sets of risks. Peters described in his table that the vulnerabilities in decentralized governance pose risks related to markets and power dynamics in the system, while P2P-networks expose the bitcoin users to the risk of double spending attack occurring. The risk of double spending can be reduced if the CPU power of the honest nodes is higher.

Netsplit attack that was mentioned in Rahouti´s article, was not mentioned in the paper that Peters published. The netsplit attack means a situation where an adversary can establish an alternative version of the blockchain by using a compromised entity. (Rahouti 2018, 67196). Conti´s paper mentions netsplit attack as well and describes it similarly to Rahouti: “an attacker creates an inconsistent view of the network (and the blockchain) at the attacked node”. (Conti 2018, 3425).

A study by Ramos S., Pianese, F., Leach, T. & Oliveras, E. examined a wide variety of operational risks. The study stated that spotting a 51% attack on a cryptocurrency requires technical skills that the public usually does not possess. The study categorizes attacks which are not reported publicly, and attacks which are reported. This kind of imperfect availability of public information may affect the market price of the attacked cryptocurrency and generate more returns for the attacker than normally possible. (Ramos et al. 2021, 12.)

From an organizational point of view peer-to-peer networks are important for a variety of reasons. P2P-networks make the entire system secure and update it consistently, making usage of the cryptocurrency safe and reliable. It is possible for the organization to reap the benefits of P2P-networks by running a node and contributing to the blockchain. It is in the organization’s interest to keep track of developments in the networks and notice changes made by the consensus.

My interpretation of the literature concerning P2P-networks and what they imply for the organizations is following: for instance, in a scenario where a netsplit or a netsplit attack happens in the way described by Rahouti, it is important for the organization to understand which direction it wants to support. Sometimes a cryptocurrency might divide in to separate blockchains when the community behind the cryptocurrency is disputing which version of the blockchain is the most feasible. These disputes can have many motives behind them, including financial, ideological, and even moral or legal. It might even be so, that the organization should re-consider which cryptocurrency to choose, if a division of blockchain happens.

Liu et al. 2021 argued that peer-to-peer nature of Over-the-Counter trade makes users susceptible to counterparty risks. (Liu et al. 2021, 37232).

Conti, M., Sandeep, K.E., Lal, C. & Ruj, S. (2018) investigated the issues of anonymity in their study. They discussed security and transaction anonymity threats which limit the applicability of bitcoins in services. Their paper is based on a comprehensive survey, which is used to provide the readers useful data who want to do research about the similar phenomena. (Conti 2018, 3417.)

To spend bitcoins, a private key is required. The bitcoins can be spent to the private key´s public key, which has a hash that acts as the address. Using this hash provides the user anonymity, and even more so if multiple addresses are used. (Conti 2018, 3418.)

It is difficult to trace transactions back to the identity of the user who initiated them. If the wallet´s address is exposed to publicity, it is possible to create more addresses to conceal the identity again. The system underlying Bitcoin improves privacy and guarantees much more anonymity than traditionally centralized financial systems, where personal data is always in the hands of an intermediary. Bitcoin´s system can provide anonymity and transparency at the same time. (Conti 2018, 3425-2426.) According to Campbell-Verduyn, Bitcoin balances between providing anonymity and transactional transparency, which can both paradoxically be sources of risks and positive features. (Campbell-Verduyn 2018, 286-287).

Peters (2016) mentioned anonymity as the fourth risk driver, which consists of sub-risks such as money laundering, fraud, legal risk, and compliance. For an organization using cryptocurrencies, anonymity can become a risk when its cryptocurrencies are stolen through fraud or other ways and the organization can´t rely on law enforcement to get their funds back when the identity of the stealer is not known. This is where the legal risk can manifest itself. Van Wegberg R., Oerlemans J.-J. & van Deventer O. made an explorative study on money laundering aspect of the crypto space. They discussed that many governments don´t recognise bitcoin as currency and therefore do not require the companies to follow "know your customer" (KYC) rules and anti-money laundering regulation. (Van Wegberg et al. 2018, 431.)

The bitcoins are very resistant against theft. The private keys used to transfer funds are not exposed when making transaction. Compared to credit cards, where the card information must be given before initiating a payment, when using bitcoins, the private key holder must never expose their private key when initiating the transaction. (Conti 2018, 3426.)

The paper mentions that there is a risk related to proper management of the private keys. Usually, the bitcoins are kept either in hardware wallet or on a wallet that is connected to the Internet. When storing bitcoins on a hardware wallet, the bitcoins are not as usable, but are more secure because they are kept off the Internet. A wallet that is connected to the Internet has more usability but is exposed to more risks. The user can also decide to keep the bitcoins on an exchange but holding them on an exchange comes with exchange-specific vulnerabilities. (Conti 2018, 3432.)

Trimborn et al. asserts that while cryptocurrencies can be kept in a “cold storage”, disconnected from any device that can be attacked, market risk is still difficult to handle and will have an impact on the value of the coins. (Trimborn et al. 2020, 281).

The Bitcoin has a function which increases the security of multi-signature wallets. It does so by employing the splitting control technique. However, the splitting technique has one severe drawback, which is that it dramatically compromises from privacy. (Conti 2018, 3428.)

The bitcoins can be stored in many ways and each of the ways come with their strengths and weaknesses. Private-key as means to access was mentioned as an operational risk in the article Peter published. While the owner of the private-key has total control over the funds it holds, it comes with arguably greater responsibility than for example holding a traditional bank account.

The publicity of transactions in Bitcoin´s blockchain can form another form of privacy risk: funds can be tracked, and the bitcoins are fungible. (Conti 2018, 3442). Therefore it is possible to track each bitcoin back to their previous addresses and even to the first time they were generated through mining. For an organization this could be a problem due to competitive reasons. Peters (2016) also mentions publicity of transaction records on the blockchain as a privacy risk. Peters highlighted a situation where there is a breach into the privacy data, and the owner of the public address is revealed to the breacher.

In a situation like mentioned above it would be possible to have an alternative way to hide identity. As Peters mentioned, implementing a system which changes address regularly after each transaction would be feasible. (Peters 2016, 263.) Conti also hinted at the possibility of multiple addresses providing more anonymity for the user. (Conti 2018, 3526). Zola et al. (2019) stated that although Bitcoin´s system is thought of as anonymous system, it is in fact pseudo anonymous. The reason it is not a full anonymous system is because it is possible to track and identify users in the Bitcoin network using their public addresses. (Zola et al. 2019, 2.) Therefore, anonymity appears in both articles as a double-edged sword, which is both beneficial for the users but at the same time comes with cons like lack of legal protection for instance.

Peters classified transaction irreversibility as one of the vulnerabilities. Transaction irreversibility is mentioned briefly in Moore´s study (2018). Irreversibility of transactions in Bitcoin makes the transaction riskier and entices scams widely in many places associated with transactions, such as mining pools, wallets, exchanges, and the illegal black market. (Moore et al. 2018, 15.)

Peters mentions in his table that the transaction irreversibility is driven especially significantly by stolen private keys that are used for making unauthorized transactions. This can lead to aggravated losses. This is a risk when using wallets and exchanges. A study by Vincent and Wilkins (2020) raises the risk regarding misidentification of a party who the transaction is sent to, causing losses because the transaction is irreversible. IT application controls which minimize the risk of misidentification can reduce the probability of it occurring. (Vincent & Wilkins 2020, 57.)

Xia et al. investigated cryptocurrency exchange scams in their article. They found out that most of the scams are controlled by a small group of attackers. (Xia et al. 2020, 15).

Publication time gap was listed as the final vulnerability mentioned in the table Peters presented. With publication time gap, Peters means the time between the execution of transaction and its time when it's published on the blockchain. Publication usually takes 10 minutes, but sometimes might take longer. These delays can make the system maintaining the cryptocurrency severely vulnerable. Frauds, double spending, and fake transactions all gain more foothold if the publication time is extended. (Peters 2016, 259.)

Saad et al. 2019 conducted a study about portioning attacks on Bitcoin. They found out that there is latency and malicious peer behaviour that leads to a lag in consensus and block propagation. In the analysis, they found out that after 5 minutes of the block´s publication, around 62,7% of nodes in the network stay behind the latest block by one or two blocks. They argued that this kind of behaviour can be exploited to create an attack where the malicious party can feed false blocks to nodes and for a short time partition the network. (Saad et al. 2019, 1175.)

The researchers managed to gather Bitcoin network information taken as samples every 10 minutes to make the analysis of consensus distribution possible each time a new block is published. They also took samples every 1 minute to investigate consensus pruning. (Saad et al. 2019, 1177.)

The paper concluded that the Bitcoin network is becoming more centralized at the AS-level, which increases it vulnerability to partioning. According to the data collected and further analysis, it is argued in the paper that the consensus pruning is non-uniform, which gives attackers opportunities to fork the network by dividing vulnerable nodes. The study mentioned four forms of partioning attacks: spatial, temporal, spatio-temporal and logical. The research seems to hint that the vulnerability is becoming a worsening issue on Bitcoin. That could be one of the reasons it gave advice for cryptocurrency exchanges to reduce the effect of these attacks. (Saad et al. 2019, 1185.)

The study is focused mostly on attacks against the blockchain networks and does not focus comprehensively on the risk of publication time gap. Peters did not use this concept of "publication time gap" anywhere else except in the table and marked it a synonym for "transaction malleability". However, he mentioned transaction malleability as one of the operational risks being caused by publication time gap. It could be interpreted that the blockchain allows both the time gap and the transaction malleability to co-exist, and they are interrelated to each other. They also cause the same risks of double spending etc. that were mentioned before.

4.4.5 Risk comparison

The new research literature on general cryptocurrency risks and bitcoin security revealed 18 separately identifiable risks compared to older literature, which revealed 15 identifiable risks. Some risks have changed over time to pose less risk to entities, other risks have disappeared, and some new risks have been discovered by other studies.

	Cryptocurrency financial risk 2013–2021		
	Risk	Mentioned before 2018?	Mentioned after 2018?
Market risks	High volatility	(Dyhrberg 2016)	(Naimy et al. 2021)
	Systemic risk	(Paech 2017)	(Ahelegbey et al. 2021)
	Systematic risk	(Paech 2017)	(Ahelegbey et al. 2021)
	Interdependency risk	No	(Aliu et al. 2021)
	Cyclical risk	No	(Aysan et al. 2021)
	Tail risk	No	(Borri, N. 2019)
Liquidity risks	Absence of regulation	(Luther 2016)	(Kirillova 2018)
	Conflict with state control	(Luther 2016)	(Renwick & Gleasure 2021)
	Lack of insurance protection	No	(Silva de Souza et al. 2019)
	Instant withdrawals	(Lin, Whinston & Fans 2015)	No
Credit risks	Exchange shutdown	(Moore et al 2013)	(Moore et al. 2018)
	Security breach	(Moore et al 2013)	(Moore et al, 2018)
	Platform risk	(Lin, Whinston & Fan 2015)	No
	Coin death risk	No	(Fantazzini 2020)
Operational risks	Decentralized governance	(Peters 2016)	(Rahouti 2018)
	Peer to peer verifications	(Peters 2016)	(Rahouti 2018)
	Transaction irreversibility	(Peters 2016)	(Vincent & Wilkins 2020)
	Anonymity	(Peters 2016)	(Conti 2018)
	Private key as mean of access	(Peters 2016)	(Conti 2018)
	Publication time gap	(Peters 2016)	(Saad et al. 2019)

Table 6. Financial risk comparison

4.2 Summarization of data from case documents

In this section of the research, I will go through balance sheets of different companies who have cryptocurrency on their balance sheets. I will be analysing, how they present cryptocurrency in their balance sheets and contrast their way of presenting it to what international accounting standards require or suggest. I will try to find and analyse similarities or differences between the balance sheet presentations and the guidance from international accounting standards. A case of Finnish Customs from Finland is included to bring different point of view to the accounting of cryptocurrencies.

4.2.1 MicroStrategy Incorporated

The first company that I am going to examine is MicroStrategy Incorporated. It provides business intelligence applications for enterprises. They held some cryptocurrency bitcoin on their balance sheet and reported the risks it exposed them to.

MicroStrategy reports that they decided to purchase and hold bitcoin as part of their Treasury Reserve policy. They may also issue debt and equity securities in capital raising transactions to purchase more bitcoin. This strategy is new and recently adopted, and the company will supervise the risks and benefits from it. The company states that the strategy has not been tested in market conditions. As a downside for the strategy the company mentions that the strategy might not be popular amongst everyone, and some investors might disagree with it. Additionally, if the strategy fails or bitcoin price goes down, it will negatively impact the market price of their class A stock. (Microstrategy 2020, 26.)

MicroStrategy held 71,079 bitcoins on February 8th, 2021, which were acquired for $1,145 billion and an average purchase price of bitcoins was 16,109 per one bitcoin including the fees. For generating cash assets as part of their treasury management, they plan to purchase more bitcoin in the future. The company states in their report that bitcoin is highly volatile, and its fair value is measured based on quoted prices taken from an exchange. (Microstrategy 2020, 26-27.)

The company makes an analysis every quarter to identify factors that could decrease the quoted prices and takes in account actual decreases in the price. This analysis is done to check whether bitcoin has impaired. To determine the impairment, the company checks the lowest price of one bitcoin and compares the carrying value of a bitcoin to it. If it exceeds the lowest price during the quarter, the company interprets it as an impairment loss. The size of impairment loss is the difference between its carrying value and the lowest price. The following increases in bitcoin price is not considered to affect the carrying value of the company´s bitcoin. Gains are not recorded until they are realized through a sale. At that point any impairment losses would count, and the gains are the net after the impairment losses. (Microstrategy 2020, 27.)

If the impairment happens, the company says it will need to incur an impairment charge, and the charge would be material to their financial results for the applicable reporting period. Bitcoins are considered digital assets in the company´s balance sheet. (Microstrategy 2020, 27.)

In the report the company covered risks related to security breaches, hacker attacks and private-key exposure. If one of these risks happen, then the company may lose some or all of their bitcoin. They further stated that security breaches and cyberattacks are concerning with respect to bitcoin. The insurance company would not cover the losses that would happen from a successful security breach or cyberattack. There is also lack of indemnity in case the custodian holding the company´s bitcoins somehow lose them. (Microstrategy 2020, 30.)

Loss of the private key and its detrimental effects to the company´s financial position is also covered in the report. To prevent the loss of the private key, the company plans to safeguard it and keep it secret. Digital wallets may be compromised when a cyberattack occurs. The company diversifies the use of the custodial services where they are holding their bitcoin due to its significant amount. The potential risk of loss is understood to be dependent on diversification. An insurance that covers a small part of their bitcoin portfolio is mentioned in the report. (Microstrategy 2020, 30-31.)

One specific risk that the company sees is that if the bitcoin is considered a security in the future. This would lead the company to be classified as an investment company under the Investment Company Act of 1940, and that comes with having to follow tighter regulatory controls which would be damaging to the financial position of the company. In addition, it would have detrimental effect on the price of the bitcoin. SEC officials do not view the bitcoin as security for now. (Microstrategy 2020, 31.)

The volatility of bitcoin and the general market is conceptualized as risky, and the company has a plan how to cope in such an environment. They plan to make an analysis every quarter to find out what could decrease the quoted prices. The analysis is for the purpose of checking whether bitcoin is likely to become less valuable. This is supplemented by impairment testing. (Microstrategy 2020, 27.)

High degree of uncertainty related to regulatory, commercial, and technical factors of bitcoin is recognised by the company. Bitcoin does not exist physically and is susceptible to technical factors related to the blockchain of Bitcoin. Some technical factors the company mentions are the following: miners might initiate malicious attacks, the blockchain might divide if it is hard forked, quantum computing might compromise the integrity of the blockchain and thus affect the price of bitcoin in a detrimental way to those investing in it. (Microstrategy 2020, 29-30.)

IAS 36 states that intangible assets require an annual impairment testing. An impairment loss can be considered to have happened when recoverable amount is below carrying amount. Microstrategy does impairment testing and measures impairment loss by calculating difference between carrying value and the lowest price. While IAS 36 requires annual impairment testing, the company seems to do testing more frequently. In this way the company follows IAS 36 standard when it comes to accounting bitcoin.

In the company´s Consolidated Statements of Operations impairment losses are called more specifically “digital asset impairment losses”. The digital assets which have impaired get written down to their fair value at the time when impairment happens. Any subsequent increases in fair value will not be adjusted to this new value. Gains are not recorded until a sale is realized. If a sale is realized, the value is presented as net of any impairment losses and recorded in the Company´s Consolidated Statements of Operations. Gain is determined by the difference of sales price and the carrying value. (Microstrategy 2020, 78.)

The company explicitly reports that it strives to do accounting in accordance with ASC 350, Intangibles – Goodwill and Other. For measurement of the bitcoin´s value, the company follows ASC 820, Fair Value Measurement. Based on quoted prices on the market in the exchange the company chose, the company measures the fair value for bitcoin (interpreted by the company as level 1 inputs). (Microstrategy 2020, 78.)

Bitcoin is part of digital assets in the company´s balance sheet and caused $70.7 million in cumulative impairment losses that was due to trading price fluctuations. (Microstrategy 2020, 12) The report contains a table which is called operating highlights. Digital asset impairment losses are recorded to be $70.7 million and are placed under “operating expenses”. (Microstrategy 2020, 42) The report calls income from these digital assets “non-GAAP income”. (Microstrategy 2020, 44.)

In the company´s balance sheet the cryptocurrency bitcoin is listed under “assets” as “digital assets”. (Microstrategy 2020, 71). Purchases of bitcoin is classified as part of “investment activities” in the cash flow statement. Impairment of bitcoin is considered as part of “operating activities”. (Microstrategy 2020, 75.)

4.2.2 Tesla, Inc.

The second company that I am going to examine is an electric vehicle and clean energy company Tesla, Inc. During 2021, Tesla has been in the news headlines for purchasing bitcoin.

Tesla reported that they purchased $1,50 billion in bitcoin during the first six months of 2021. Bitcoin was accepted as payment for certain products during the first three months, but it was no longer accepted in May 2021. However, Tesla stated that they might accept bitcoin again as payment for products and services in the future. Tesla calls cryptocurrencies “digital assets” in their report. If cryptocurrency is used for payment, Tesla will account for non-cash consideration according to the standard set in ASC 606, Revenue from Contracts with Customers. Quoted market price of the digital asset at the time of the payment is accepted. (Tesla 2021, 15.)

On the consolidated balance sheets digital assets are classified under assets with the net value of $1,31 billion. (Tesla 2021, 8). On the consolidated statements of cash flows which shows the financial data from 30th June 2021, Tesla recorded purchases of digital assets for $1,5 billion in cash flows from investing activities and digital asset gain of $78 million in cash flows from operating activities. The statements are unaudited. (Tesla 2021, 9.)

In accordance with ASC 350 – Intangibles, Goodwill and Other, all digital assets are accounted as indefinite-lived intangible assets. Third parties might be used to host custodial services for holding the digital assets, but Tesla still owns and controls its bitcoins in these services. The digital assets are recorded first at cost and remeasured for presentation on consolidated balance sheet at net cost of possible impairment losses. (Tesla 2021, 15.)

They determine the fair value of their digital assets on nonrecurring basis and in accordance with ASC 820. Tesla determines active exchanges as principal market for digital assets (as level 1 inputs). They make a quarterly analysis on the quoted prices taken from these exchanges and determine whether the prices have decreased, which would indicate that the digital assets have impaired. (Tesla 2021, 15.)

When there are impairment losses, they are recognized within Restructuring and other in the statement about operations. The recognition happens in the same period impairment happened. The impaired digital assets are presented according to their fair value at the time of impairment. If the digital asset increases in value after this, it is not written down. (Tesla 2021, 15.)

On the time span of six months until 30th June 2021 Tesla had purchased $1.50 billion of bitcoins. In March 2021, Tesla realized gains of $128 million. Tesla also incurred losses of $73 million later up until June. The carrying value of bitcoins held by Tesla was $1.31 billion and the fair market value was $1.47 billion on 30th June 2021. (Tesla 2021, 17.)

Considering the fact that Tesla reported that they determine the fair value on nonrecurring basis, Tesla´s investment in bitcoins seems to have been a one-time phenomenon for now. Tesla mentions on their report that they believe in the long-term potential of digital assets as an investment possibility and a liquid alternative for cash. (Tesla 2021, 54.) There seems to be enough confidence to acknowledge that the benefits of investing in bitcoin might outweigh the risks to justify the significantly large sum Tesla invested. Funds that were not needed to fulfil adequate liquidity, were invested in different commodities, one of them being bitcoin. (Tesla 2021, 54) Investment in bitcoin was seen as a good diversification option. (Tesla 2021, 54.)

It is acknowledged in the report that digital assets can be highly volatile. Digital assets lack a physical form and rely on technology in everything. Decentralization may subject the digital assets to malicious attacks. The report also mentions risks associated with regulation. Laws on securities might change in the future. GAAP might require changing the way how digital assets are accounted, which Tesla also notes as risk. (Tesla 2021, 54.)

Because there are no centralized bodies, digital assets may be susceptible to security breaches and other such activities. Human errors might result in losing private keys required to control the wallet where bitcoins are. Tesla reports taking all these risks into account by taking measures to secure digital assets if the risks are realized. (Tesla 2021, 54.)

Volatility of bitcoin might cause challenges when the company wants or needs to liquidate the investment. Having to liquidate at unfavourable time when the bitcoin´s price is low is a liquidity risk arising from volatility. (Tesla 2021, 42.) Earlier it was mentioned in Fantazzini´s study, that market risks and credit risks are more interrelated in cryptocurrencies. This seems to be the case to some extent with liquidity risk as well if the liquidity risk is understood as how it was defined by Christoffersen.

Judging from the report, Tesla appears to follow internationally recognised accounting standards when it comes to accounting of bitcoin. As previously mentioned, Tesla determines cryptocurrencies as intangible assets, following ASC 350 Intangibles – Goodwill and Other. Tesla has other intangible assets in addition to bitcoin, and seemingly for this reason has a separate line item specifically for bitcoin called "digital assets". This is separate distinction was also made between digital assets and intangible assets in the balance sheet. Tesla states that digital assets are considered intangible assets according to the recognised accounting norms. (Tesla 2021, 34.)

4.2.3 The Finnish Customs

Cryptocurrencies are treated differently in the Finnish government agencies. I am taking the Finnish Customs as a case where cryptocurrencies are viewed differently compared to the American and European companies. Crypto assets are most often obtained through law enforcement actions and are not utilized actively. This differing accounting treatment and perception is examined in this case.

The Finnish Customs is in close co-operation with other agencies, probably the most relevant being the Finnish State Treasury. In fact, the State Treasury gives agencies instructions on how to do accounting in exceptional cases, which is why it is important to bring the State Treasury´s instructions on cryptocurrencies to the light in this study.

About accounting of cryptocurrencies according to Finnish State Treasury. The Finnish State Treasury has given instructions about accounting of cryptocurrencies. Most often the reason the state agency has obtained cryptocurrency is related to foreclosure or confiscation related to suspicion of crime. Because of these reasons, accounting department might have obtained an accumulation of cryptocurrencies over time. (State Treasury 2018, 2.)

These are cryptocurrencies that the accounting departments don´t use for doing payments, don´t invest in them and don´t accept them when receiving payments. Usually, exceptions are made when the cryptocurrency is obtained through crime prevention purposes. The State Treasury instructs to hold the cryptocurrencies until more court decisions and laws are issued regarding the handling of cryptocurrencies. By norm, the cryptocurrencies are either returned to their original holders, are sold to meet liquidity requirements, or are sentenced to be lost to state. (State Treasury 2018, 2.)

The government doesn´t treat cryptocurrencies as official currencies. Instead, they are treated as assets. Cryptocurrencies confiscated by the government are not moved to accounting before there is a court decision about judging such asset to be lost to the state. Before such decision is made, the asset is recorded according to the law which is underlying the confiscation. For assets obtained through foreclosure, there is specific regulation regarding foreclosures. (State Treasury 2018, 2.)

In the year 2019 the Finnish Customs had 10,8 million EUR worth of bitcoins in possession. By the 31st of December 2020 the Finnish Customs held 1980,8 bitcoins. The bitcoins are handled as a distinct asset class and are recorded in the accounting documents after the confiscation. The agency follows instructions from the State Treasury. According to the document, 1889.1 bitcoins were sentenced to be lost to the state. (Finnish Customs 2021, 28-29.)

The Finnish Customs did not record the appreciation of cryptocurrencies to balance sheet. (Finnish Customs 2021, 28) However, on the annual report, the cryptocurrencies were presented under investments as “other investments” on appendix 10. (Finnish Customs 2021, 49.)

The Customs in Finland seems to value cryptocurrencies similarly to securities, because they are valued as “other investments” in the annual report. This is in line with the Finnish Accounting Board´s interpretation, where cryptocurrencies should be valued as “other stocks” or “other investments”. The agency did not extensively report risks associated with cryptocurrencies.

The international accounting standards such as IFRS and FASB are not mentioned in the annual report, most likely due to the nature of the organization as a government agency and the accounting style in Finland. Instead, the agency seems to follow the Finnish Accounting Act of 1997 and the Accounting Board´s recommendations.

4.2.4 Bitcoin Group SE

Bitcoin Group SE is a German venture capitalist firm, which helps companies to grow by providing them with capital and management services. It is focused on companies that deal with cryptocurrencies and blockchain technology.

They reported that there is an operational risk against using cryptocurrencies related to hackers or employees potentially being able to steal the crypto assets entrusted to the subsidiary company called futurum bank AG. These crypto assets are the funds of the customers using the service and losing these funds would mean that the company would have to reimburse any funds lost due to the manifestation of the operational risks. It would also have a negative long-term impact on the company´s financial position. (Bitcoin Group 2020, 32)

Cryptocurrencies, called intangible assets in the company´s balance sheet, increased in total from EUR 27,506 to EUR 90,307. The company reports intangible assets as non-current assets. (Bitcoin Group 2020, 27.) Cryptocurrencies are reported separately from other intangible assets in the company´s financial statements. (Bitcoin Group 2020, 74). Intangible assets also include purchased software, domains, and banking licenses. Cryptocurrencies are reported at their revaluation value, which is measured as fair value, where cumulative impairment expenses are deducted from. The fair value is determined by referring to an active market. (Bitcoin Group 2020, 60.)

The company measures fair value according to IFRS 13 “Fair Value Measurement”. (Bitcoin Group 2020, 89). But this is not the standard company uses for cryptocurrencies. The fair value is determined by checking annual impairment of crypto assets, and the company reports it is following IAS 36. (Bitcoin Group 2020, 60.)

Bitcoin Group SE follows international accounting standards when it values cryptocurrency.

4.2.5 Argo Blockchain

The fifth case will be focusing on Argo Blockchain, which is a crypto mining service provider that is based in the UK. Argo Blockchain has a listing on the main market of London Stock Exchange. As the company is providing crypto mining services to the consumers, it naturally has cryptocurrencies on the balance sheet itself. Therefore, it will make a good candidate for being the second European company that will be examined in this case study.

Cryptocurrencies are called "Digital assets at fair value through profit or loss" in the company´s statement of financial position and classified as "current assets". The company holds £4 637 438 worth of digital assets on 31st December 2020. (Argo Blockchain 2021, 32.) The company gets income from mining cryptocurrencies and follows IAS 2 Inventories due to its acting as a commodity-broker as defined IAS 2 Inventories. (Argo Blockchain 2021, 39-40).

The cryptocurrencies are stated to not qualify as cash or financial assets. Because the company is using cryptocurrencies as a commodity broker, the changes in fair value of digital assets is reported as a profit or loss. (Argo Blockchain 2021, 40.) Argo Blockchains classified held cryptocurrencies to level 1 inputs in the fair value hierarchy. (Argo Blockchain 2021, 47).

The biggest general risks are reported to be high volatility in the cryptocurrency market, uncertainty, and general sentiment of the market. Most of the company´s assets are stored in bitcoins and to mitigate the volatility risk, the company actively monitors its portfolio of digital assets. Extreme price changes stemming from the volatility might render the company unable to sell the assets without losing purchase power, which is a liquidity risk but stated in other words. The company reports security breaches as a risk that could lead into loss of the digital assets the company holds. To mitigate this risk, the company uses the services of a third-party custodians that have security measures to deal with the risk. (Argo Blockchain 2021, 10.)

Market risk arising from volatility of cryptocurrencies is mentioned again and this time under the chapter of "Financial Risk Management" in the report. The company claims that foreign exchange rates also affect the market risk. The credit risk is reported to be low because the reserves are held in "credible institutions". The report states that the company is potentially vulnerable to liquidity risk and capital risk arising from having to purchase hardware for crypto mining operations. These risks are mitigated by adequate portfolio management and through maintaining a working capital. (Argo Blockchain 2021, 16.)

The report states that a risk of fraud originating from material misstatement of the financial statements is possible. There is a risk related to valuation of crypto assets which could be subject to management bias. The digital assets held at the end of the year were classified as “level 2” in the fair value table. Supporting evidence from a trading platform was gathered to support the fair value that was assigned to the crypto assets. (Argo Blockchain 2021, 29.)

Two most significant risks with correct presentation of cryptocurrencies are the high volatility and the high need of management estimates. Both factors can lead to material misstatement of cryptocurrencies. (Argo Blockchain 2021, 27.)

The annual report did not include a comprehensive balance sheet. The report was made up of separate financial statements, which did not interpret bitcoin as security, but a commodity.

4.2.6 Analysis table

Some organizations in the cases are very different from others in the way they operate and how they use cryptocurrencies. Therefore, I have gathered the essential information from the cases analysed above. Below is a table demonstrating the summary of the cases above.

Organization	Document Name	Crypto valued as	Valuation regulation	New Risks
MicroStrategy Inc	2020 Annual Report	Commodity	IAS 36 impairment test, ASC 820	Quantum Computing
Tesla Inc	Form 10-Q	Commodity	ASC 820, ASC 606 & ASC 350	Adoption risk
Finnish Customs	Tullin tilinpäätös vuodelta 2020	Investment / N/A	KILA 1895/3.7	-
Bitcoin Group SE	Annual Report 2020	Commodity	IFRS 13, IAS 36	-
Argo Blockchain	Annual Report Accounts	Commodity	IAS 2	Material misstatement

Table 7. Valuation analysis.

The table has the column called “New Risks”. This column means new risks which appeared in the annual reports but did not appear in the literature analysed in the systematic literature review. Valuation of cryptocurrency is typified into categories of “Commodity” and “Security”. This is my own interpretation of annual reports, based on the companies’ views on cryptocurrency being a commodity or a security. The Finnish Customs did not provide an exhaustive perspective on whether the cryptocurrency should be valued as a commodity or a security, hence I drew my conclusions from the KILA 1895/3.7 and the Finnish accounting law that the Finnish Customs follows over international accounting standards. The conclusion is also based on the appendix where the Finnish Customs valued their bitcoins as “Other Investments”.

5. RESULTS

5.1 Literature Synthesis

Overall, the knowledge of cryptocurrency risks has increased dramatically after the year of 2017. Research literature on the topic of cryptocurrencies has also multiplied in the years of 2018-2021 when compared with 2013-2017. Most of the risks have stayed over time, and there are some new risks which emerge from the newer literature. Some risks have less impact on cryptocurrencies as they did before 2018, and there are even risks which have completely disappeared from the newer literature.

Because some risks have less impact on cryptocurrencies than before, and the risks and how to mitigate them are understood better, it can be considered that the second hypothesis is true. Cryptocurrency risks have decreased and are likely to decrease in the future when new regulation is enacted and the market with its blockchain technology increases in size, doing away with many of credit risks. Cryptocurrencies are still highly speculative, and many governments might end up banning it.

The volatility of cryptocurrencies is the most mentioned risk, which is interrelated to other risks. Systemic risk can be defined in different ways, but as a market risk it is most understood to be the risk coming from the financial system in the context. After the crypto bubble of 2018, the researchers increasingly noticed more risks in the market. They started to pay attention to the cyclical element of the crypto market, which can pose a cyclical risk and interdependency of cryptocurrency prices.

Different studies might use the same concepts but define the concepts differently. Credit risk is a concept which is defined differently, depending on the study. Borders between different risk concepts can be flexible, as for instance credit risk and market risk are commonly interrelated.

Even though there appears to be more risks in the literature after 2018, it does not mean that the quantity of risks has necessarily increased. There have been more studies on cryptocurrency risks after 2018, which had led to better understanding of risks and discovery of more risks. Many risks which have existed before 2018, exist still, but the maturation of cryptocurrency markets might have reduced the impact of these risks.

Exchange shutdown risk is less likely to impact an exchange which has been around for several years, than a new exchange. Volatility is seen traditionally as a big risk with cryptocurrencies, but market capitalization of bitcoin and other altcoins is now many times bigger than it was before 2018, making tremendous negative or positive corrections that happened in the crypto bubble of 2018 less likely to happen. While Moore´s indicated that bigger exchanges are more likely to be breached, the probability of an exchange being breached topped in the years of 2013-2014 and declined from there on. Investing in bigger exchanges should now be less risky than before when they are not breached as frequently as before and have lower shutdown risk due to their existence over long period of time.

With new cryptocurrencies on the other hand, there is a coin death risk that does not exist when it comes to the most established coins. Studies are acknowledging cryptocurrencies as attractive portfolio diversification opportunities, and that shifts attention to entirely new kind of risks. For example, lack of insurance protection is seen as a risk. Platform risk did not appear in the newer literature.

Cryptocurrency benefits depend on in what context they are used. If they are used for investment activities, there are multiple researchers who confirm that cryptocurrencies are highly useful for portfolio diversification. Regardless of the use, financial risk can be said to be of high importance to many who use cryptocurrencies. Therefore, to answer the first hypothesis, whether reduction in financial risk has increased the benefits of using cryptocurrencies, the answer would be, slightly. It would be too early to say whether financial risk has decreased enough to significantly increase benefits of using cryptocurrencies, because new risks have appeared which need more research. Most reductions in risks happened in the credit risk category.

Systematic risk causing the entire crypto market to take a deep dive similarly to crypto bubble bursting in 2018 is less likely in 2021 but might still happen. High volatility has not disappeared from the crypto markets, but positive and negative shocks affecting it are now understood better.

The lack of regulation is still seen as an issue in the studies, but there has been more regulation put in place after 2018. Regulation has increased over the time: some exchanges are even voluntarily doing KYC (Know Your Customer) identifications and in some countries a license is required to run a crypto exchange. The governments are not rushing to regulate the field as it is new, and many innovations can still take place, which the government doesn´t want to stop with early regulation. Interestingly, the liquidity risk focus on the crypto market has changed over time. Instant withdrawals were seen as a liquidity risk causing issue in the older study, but it was not mentioned in the new studies. Lack of insurance protection was discovered as a new risk mentioned in newer study.

While earlier study by Luther viewed the risk of conflict with state control in the context of government resorting to ban cryptocurrencies, later study by Renwick observed it from the context of government purposely delaying imposing regulation to not have detrimental effect on the innovation. Bitcoin has had a reputation in the past as a currency used for illegal activities, and it would not have been an unlikely occurrence for the governments to start banning it. Over time, bitcoin has had more attention to it as an investment and payment method, which could explain why many governments see the potential in bitcoin and refrain from outright banning it.

Many of the operational risks have stayed the same as the technology is the same as it was before 2018. Blockchains are decentralized and are always exposed to risks coming from not having a centralized authority confirming the legality and morality of transactions. This also has to do with transaction irreversibility. There is larger variety of scams and frauds when the cryptocurrencies are in a "bull-run" phase. Transaction irreversibility causes many other risks: it makes misidentification much more punishing and entices many scams and frauds when funds can't be retrieved once they are sent. Hence more is at stake as a centralized safeguarding authority does not exist and funds can't usually be manually retrieved if they are sent to wrong address.

While the technology behind the cryptocurrencies is decentralized, the users still must buy their cryptocurrencies from somewhere. This most often involves having to interact with an exchange, which is centralized. This could lead to situations that are not intended to happen with decentralized cryptocurrencies. The exchange could suffer from a security breach, which could put the customer´s funds under risk.

Different cryptocurrencies are using different consensus mechanisms and blockchains to make transactions possible. These consensus mechanisms come with their own strengths and drawbacks. Bitcoin is based on a consensus mechanism that requires a majority in the network. This has a drawback that if an attacker manages to get a majority, then the attacker could theoretically modify the blockchain to include transactions that would otherwise have never happened. Even though this is extremely unlikely due to the tremendous hardware and electricity investments that would need to be done, this can serve as an example how catastrophic event it would be if it happened.

Bitcoin provides both anonymity and transactional transparency. This is a paradoxical set-up, that exposes the entity to risks. For an organization the anonymity can come up as a negative feature if the crypto assets are stolen and law enforcement is unable to protect the organization´s assets due to the anonymous addresses on the blockchain. Transactional transparency might be a down-side if the organization wants to keep its transactional activity a secret.

Publication time gap is another risk that is related to the technology the Bitcoin is using. The peers in the network are given 10 minutes to confirm transactions, and this time gap could be exploited by attackers. This can let the attackers use portioning attacks for instance.

5.2 Results from case data

The research investigated 5 different cases. Two of the cases were American companies, two of them European and one was a government agency from Finland. All the companies followed either IFRS or FASB standards, or both. Tesla Inc. followed instructions set by FASB when it valued cryptocurrency in its balance sheet. When it comes to valuation of cryptocurrencies, most companies used the fair value hierarchy set by the international accounting standards. Bitcoin Group SE conducted annual impairment testing instructed by IAS 36 but did not use the fair value hierarchy framework. The Finnish Customs did not directly follow international accounting standards, instead it followed local accounting law and accounting board´s interpretation.

The Finnish customs decided to not include the appreciation of crypto assets in the balance sheet in its 2020 annual report. The agency presented the crypto assets in a separate appendix as “other investments”, following the accounting board´s recommendation directly.

The companies differed vastly on how they used crypto assets and where they obtained the cryptocurrencies from. Tesla used up extra liquidity that would not affect the adequate liquidity held for regular operations and invested it in bitcoin for short-term. Microstrategy on the other hand is holding bitcoins as its primary treasury asset. Bitcoin Group SE provides a marketplace, where cryptocurrencies can be traded. For this purpose, it holds small portion of its bitcoins ready for trading activities. It keeps rest of its cryptocurrencies in offline storage. Argo Blockchain is a mining service provider which mines itself as well. The Finnish Customs has accumulated cryptocurrencies because of law enforcement activity such as confiscations.

Volatility and uncertainty of the market were the most mentioned risk-inducing factors. Having to rely on third party custodians who have access to the funds was also commonly mentioned risk-inducing factor.

The American companies MicroStrategy and Tesla reported loss of public-private keys as one of the fundamental operational risks. Lack of insurance protection, which appeared as a new risk in the literature review, was mentioned as a risk by MicroStrategy. The possibility of a security breach, which would expose the stored funds to the attackers, was reported as an operational risk by both American companies and also by Argo Blockchain, a European company.

Tesla and Argo Blockchain called their cryptocurrencies digital assets in their annual reports, which it is a synonym for intangible asset. Argo blockchain valued cryptocurrencies as level 1 in the fair value hierarchy table, and Tesla considers them level 1 inputs as well. Microstrategy values cryptocurrency similarly to Tesla, as level 1 inputs. Bitcoin Group SE follows IFRS standards on valuation of non-financial, intangible assets. Therefore, the company reports cryptocurrencies as intangible, non-financial assets. It does not use value hierarchy for crypto assets, instead it determines the value with annual impairment testing stated in IAS 36.

The cryptocurrency is valued in all companies as an intangible asset and a commodity. Cryptocurrency is not viewed as a security or a stock in any company´s annual report. In fact, interpretation of cryptocurrencies as securities by regulators in the future is seen as a risk by some of the companies. The answer to third hypothesis is true.

5.3 Intersection of results

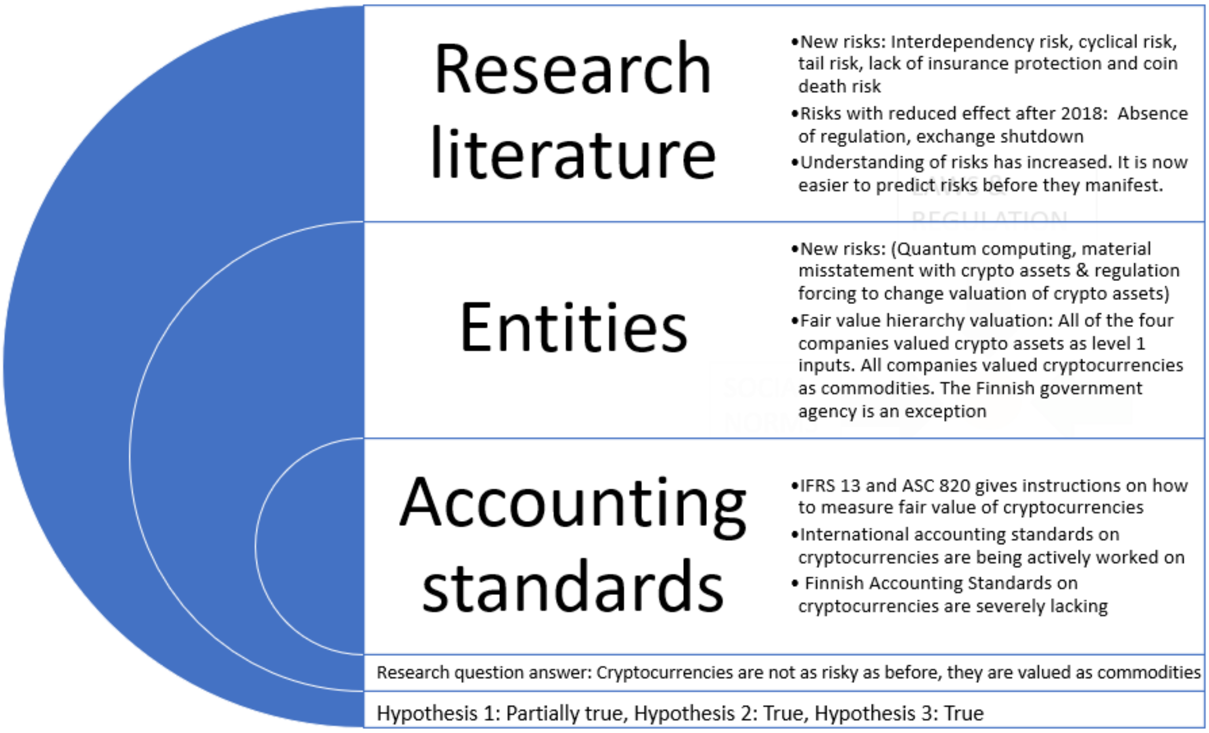

Figure 8. Intersection of results.

The research results could be understood in the way presented in the figure above. The international accounting standards are at the core of the study, which explain risk reporting and cryptocurrency valuation in the entities. The entities can be observed to understand risks that come up in the research literature. The observation can also be done vice-versa: research literature can describe risks which appear in reporting of the entities, and the risks and valuation decisions done in the entities can be observed to see the direction where the accounting standards attempt to direct.

The larger the sphere, the more coverage it gives for understanding the cryptocurrencies. The research literature in this case, being the largest sphere, mentions 5 new risks which emerged from the literature. It also gives answers to the first and second hypothesis: risks have reduced after 2018 and it is easier to predict risks making investing in cryptocurrencies more beneficial. The research question on part of the riskiness of crypto assets is thereby clearer: cryptocurrencies are not as financially risky as they were before.

The entities are in the middle of the figure and are affected by the international accounting standards and the various risks detected in the research literature. Some entities mentioned new risks that were not directly mentioned in the research literature. Development of quantum computing for example, could be a risk that would have tremendously negative consequences for long-term investments in cryptocurrencies. If the governments change the regulation to force the entities to value cryptocurrencies as securities, it will have very negative consequences for the financial positions of entities investing in cryptocurrencies.

All companies value the fair value of cryptocurrencies as level 1 inputs. All companies are therefore taking the fair value from the market prices, which seems to set consensus on how the fair value of cryptocurrencies could be valued. Annual report of Argo Blockchain mentioned material misstatement related to wrong interpretation of these fair value hierarchy inputs by the management as a risk. The Finnish government agency did not follow international accounting standards as baseline; therefore, it can be considered an exception.

There are some general guidelines in international accounting standards how to measure impairment of digital assets. This can be applied to crypto assets, and the companies have. IAS 36 gives important instructions on how impairment is measured, and ASC 820 alongside with IFRS 13 instructs on fair value measurement. Alternatively in the Finnish government, KILA 1895 and the Finnish Accounting Act of 1997 is followed. It is important to note that instructions given by the international accounting standards are actively being worked on at the time of making this study.

All the companies valued cryptocurrencies as commodities, and further categorized them to different categories in annual reports and balance sheets depending on their use. Bitcoin Group SE put cryptocurrencies in to "non-current assets" and Argo Blockchain put them in to "current assets". Microstrategy listed cryptocurrencies under "assets" and "digital assets". Tesla classified cryptocurrencies to digital assets as well. Judging from these cases, the third hypothesis is true. Taking in account that the case companies valued cryptocurrencies as mentioned, the research question is now fully answered. Cryptocurrencies are valued as commodities, and they are not as financially risky as they were before.

6. CONCLUSIONS

The goal of the study was to understand how international accounting standards affect cryptocurrency´s valuation on balance sheets of different organizations. The study contained case studies of varied organizations and a systematic literature review on academic literature discussing risks of using cryptocurrencies.

Recent academic literature indicated that there is now a better understanding of risks and benefits related to cryptocurrencies. Many risks which existed in newer and older literature have reduced impact on the financial risk posed by cryptocurrencies. For instance, many cryptocurrency exchanges are now safer to use, early warning signals can be detected before systematic risk manifests and regulatory oversight is becoming stronger. Due to these factors, the second hypothesis is true, and the first hypothesis is partially true. While weakening of some risks have decreased financial risk of cryptocurrencies, new risks have been discovered and more research is needed on them.

Cryptocurrencies are gaining more relevancy, and this has led to discussions in FASB and other accounting organizations. Companies included in the case studies viewed cryptocurrencies as digital commodities. This kind of view is in line with the interpretation of international accounting standards seeing cryptocurrencies as intangible, digital assets which are not considered financial assets similarly to feat currencies. They were not seen as securities either. This answers positively to the third hypothesis on whether the cryptocurrencies are valued in the balance sheet similarly to commodities. Answers to all hypotheses seem to indicate, that the answer to the research question is the following: Cryptocurrencies, valued by case companies as commodities, are not as risky as before, but need more research before further conclusions on risk-benefit ratio can be made.

Benefits of cryptocurrencies include portfolio diversification, lack of intermediaries and transparency. Bitcoin is very weakly correlated with traditional asset classes, which makes it a useful portfolio diversification asset. Apart from using an online exchange, there are no intermediaries. Lack of middlemen can potentially reduce costs for entities using bitcoin. All transactions are public and viewable by anyone on the Bitcoin blockchain. This publicity makes the whole ecosystem very transparent. Paradoxically, it could be a negative trait if the entity´s public key is exposed. This could let anyone see all bitcoin transactions the entity is making, including competitors. There is some degree of anonymity provided by the blockchain, but the user is responsible to keep public and private keys secret. Exposure of public key would let anyone know the identity of the user behind the public, and the loss of private key would mean possible loss of funds.

Reliability of the study is increased by the fact that it is very repeatable. The systematic review is described with its all steps in the methods, and the documents used in the case studies are listed and publicly available. Validity is affected by lack of comprehensive research literature on cryptocurrency risks and the yet-developing international accounting standards that this study investigated. Older studies did not discover some risks which existed back then, which newer studies did. A challenging factor for the validity was that there was very little regulation on accounting of cryptocurrencies in Finland. This is likely to change in the future, which is why I recommend conducting new studies on this same topic after the change in accounting regulation happens.

Researchers are still studying the cryptocurrency risks very actively in this field which is full of literature gaps. More research is needed for the definition of the concepts of credit risk and liquidity risk in the context of cryptocurrencies. Bitcoin is just one of the many cryptocurrencies that has its own utility and blockchain, therefore there is a need for more studies on other cryptocurrencies than bitcoin and how they are valued. Some companies reported government´s possible future regulation on cryptocurrencies as a risk if the government decides to value cryptocurrencies as securities rather than digital commodities.

SOURCES

Ahelegbey, D.F., Giudici, P. & Mojtahedi, F. 2021. Tail risk measurement in crypto-asset markets. International Review of Financial Analysis, 73, art. no. 101604

Alfieri, E., Burlacu, R. & Enjolras, G. 2019. On the nature and financial performance of bitcoin. Journal of Risk Finance, 20 (2), 114-137.

Aliu, F., Nuhiu, A., Krasniqi, B.A. & Jusufi, G. 2021. Modeling the optimal diversification opportunities: the case of crypto portfolios and equity portfolios. Studies in Economics and Finance, 38 (1), pp. 50-66.

Aysan, A.F., Khan, A.U.I., Topuz, H. 2021. Bitcoin and altcoins price dependency: Resilience and portfolio allocation in covid-19 outbreak. Risks, 9 (4), art. no. 74, 1-13

Borri, N. 2019. Conditional tail-risk in cryptocurrency markets. Journal of Empirical Finance, Iss. 50, 1-19

Brown, Gavin & Whittle, Richard 2020. Algorithms, blockchain & cryptocurrency : implications for the future of the workplace. Bingley, England : Emerald Publishing

Brown-Hruska, S. & Wagener, T. 2018. The virtual currency regulatory framework in global context. Capital Markets Law Journal, 13 (4), 487-517

Burilov, V. 2019. Regulation of Crypto Tokens and Initial Coin Offerings in the EU: De lege lata and de lege ferenda. European Journal of Comparative Law and Governance, 6 (2), 146-186

Campbell-Verduyn, M. 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change, 69 (2), 283-305.

Christoffersen, Peter 2011. Elements of financial risk management. San Diego: Elsevier Science & Technology. 3-4

Conti, M., Sandeep, K.E., Lal, C. & Ruj, S. 2018.
A survey on security and privacy issues of bitcoin IEEE Communications Surveys and Tutorials, 20 (4), art. no. 8369416, 3416-3452.

De Filippi, Primavera De Filippi 2018. Blockchain and the Law: The Rule of Code. Cambridge: Harvard University Press

Fantazzini, D. & Zimin, S. 2020. A multivariate approach for the simultaneous modelling of market risk and credit risk for cryptocurrencies. Journal of Industrial and Business Economics, Vol 47 (1), 19-69.

Dyhrberg Anne Haubo 2016. Bitcoin, gold and the dollar – A GARCH volatility analysis. Financial Research Letters. Vol 16. 85-92

Eyal, Ittay. 2017. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. Vol 50. No 9 38-49

Gandal, N., Hamrick, J.T., Moore, T., Oberman, T. 2018. Price manipulation in the Bitcoin ecosystem. Journal of Monetary Economics, 95, 86-96.

Grover P, Kar AK. & Janssen M. 2019. Diffusion of blockchain technology. Journal of Enterprise Information Management. Vol 32 No 5 735-757

Hasanova, H., Baek, U.-J., Shin, M.-G., Cho, K., Kim, M.-S. 2019.
A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29 (2), art. no. e2060, 1-27

Hassija V., Chamola V., Gopala K., Dara N., Kumar N. & Guizani M. 2021. A Blockchain and Edge-Computing-Based Secure Framework for Government Tender Allocation. IEEE internet of things journal. Vol 8 No 4 2409-2418

Hempfing, A. 2019. What's left after the hype? An empirical approach comparing the distributional properties of traditional and virtual currency exchange rates. PLoS ONE, 14 (7), art. no. e0220070, 1-21

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita . 13. osin uud. laitos. Helsinki: Tammi, Print.

Hui, C.-H., Lo, C.-F., Chau, P.-H. & Wong, A. 2020.
Does Bitcoin behave as a currency?: A standard monetary model approach. International Review of Financial Analysis, 70, art. no. 101518, 1-12

Kirillova, E. A., Pavlyuk, A. V., Mikhaylova, I. A., Zulfugarzade, T. E., & Zenin, S. S. (2018). Bitcoin, lifecoin, namecoin: The legal nature of virtual currency. *Journal of Advanced Research in Law and Economics, 9*(1), 119-126.

Knittel, M., Pitts, S. & Wash, R. 2019. "The most trustworthy coin": How ideology builds and maintains trust in bitcoin. Proceedings of the ACM on Human-Computer Interaction, 3 (CSCW), art. no. 36, 5-6

Kostika, E. & Laopodis, N.T. 2020. Dynamic linkages among cryptocurrencies, exchange rates and global equity markets. Studies in Economics and Finance, 37 (2), 243-265

Lin Zhangxi, Winston Andrew B, Fan Shaokun. 2015. Harnessing internet finance with innovative cyber credit management. Financial Innovation (Heidelberg), Vol 1, 1-24

Liu, X.F., Jiang, X.-J., Liu, S.-H. & Tse, C.K. 2021. Knowledge Discovery in Cryptocurrency Transactions: A Survey IEEE Access, 9, art. no. 9364978, pp. 37229-37254.

Luther, WJ. 2016. Bitcoin and the Future of Digital Payments. The Independent Review Vol 20. Iss. 3 397-404

Malladi, R.K. & Dheeriya, P.L. 2021. Time series analysis of Cryptocurrency returns and volatilities. Journal of Economics and Finance, 45 (1), 75-94.

Moore, T., Christin, N. & Szurdi, J. 2018. Revisiting the risks of bitcoin currency exchange closure ACM Transactions on Internet Technology, 18 (4), art. no. 50

Moore Tyler & Christin Nicolas 2013. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. International Conference on Financial Cryptography and Data Security. 25-33

Naimy V, Haddad O, Ferna´ndez-Avile´s G, El Khoury R (2021). The predictive capacity of GARCH-type models in measuring the volatility of crypto and world currencies. PLoS ONE 16(1): e0245904. https://doi.org/10.1371/journal. pone.0245904

Osterland, Thomas & Rose, Thomas. 2020. Model checking smart contracts for Ethereum. Pervasive and Mobile Computing Vol 63 1-11

Othman, AHA., Abdullah, A. & Haron, R. 2019. Are the new crypto-currencies qualified to be included in the stock of high quality liquid assets? A case study of bitcoin currency. Al-Shajarah: Journal of The International Institute of Islamic Thought and Civilization (ISTAC)

Paech, P. 2017. The Governance of Blockchain Financial Networks. Modern law review. Vol 80 (6) 1073-1110

Peters, G. W., Chapelle A. & Panayi E. 2016. Opening discussion on banking sector risk exposures and vulnerabilities from Virtual currencies: An Operational Risk perspective. Journal of Banking Regulation. Vol 17. Iss 4. 239-272

Rahouti, M., Xiong, K. & Ghani, N. 2018. Bitcoin Concepts, Threats, and Machine-Learning Security Solutions IEEE Access, 6, art. no. 8528406, 67189-67205

Ramlall, I. 2019. Economic Areas Under Financial Stability. First edition. United Kingdom: Emerald Publishing Limited. eBook.

Ramos S., Pianese F., Leach, T. & Oliveras E. 2021. A great disturbance in the crypto: Understanding cryptocurrency returns under attacks. Blockchain: Research and Applications.

Renwick, R., Gleasure, R. 2021. Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. Journal of Information Technology, 36 (1), 16-38.

Saad, M., Cook, V., Nguyen, L., Thai, M.T., Mohaisen, A. 2019. Partitioning attacks on bitcoin: Colliding space, time, and logic Proceedings - International Conference on Distributed Computing Systems, 2019-July, art. no. 8884930, 1175-1187

Saiedi E., Broström A. & Ruiz F. 2021. Global drivers of cryptocurrency infrastructure adoption. Small business economics. Vol 57 Iss 1 353-406

Sifat I. 2020. On cryptocurrencies as an independent asset class: Long-horizon and COVID-19 pandemic era decoupling from global sentiments, Finance Research Letters, Vol 43

Silva de Souza, M.J., Almudhaf, F.W., Henrique, B.M., Silveira Negredo, A.B., Franco Ramos, D.G., Sobreiro, V.A. & Kimura, H. 2019. Can artificial intelligence enhance the Bitcoin bonanza. Journal of Finance and Data Science, 5 (2), 83-98

Trimborn, S., Li, M. & Härdle, W.K. 2020. Investing with Cryptocurrencies - A Liquidity Constrained Investment Approach. Journal of Financial Econometrics, 18 (2), 280-306.

Tu C, D'Odorico P. & Suweis S. 2020. Critical slowing down associated with critical transition and risk of collapse in crypto-currency. R. Soc. open sci.

Umar M., Syed Rizvi, S. & Naqvi B. 2021. Dance with the devil? The nexus of fourth industrial revolution, technological financial products and volatility spillovers in global financial system, Technological Forecasting and Social Change, Vol 163

van Wegberg, R., Oerlemans, J.-J., van Deventer, O. 2018. Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. Journal of Financial Crime, 25 (2), 419-435.

Vinayak, Muskan, Paal Singh Panesar & Har Amrit. 2018. Analyzing Financial Smart Contracts for Blockchain. International Conference on Internet of Things. 1701-1706.

Vincent, N.E., Wilkins, A.M. 2020. Challenges when auditing cryptocurrencies. Current Issues in Auditing, 14 (1), A46-A58.

Weiyi, C. 2018. Disruption of financial intermediation by FinTech: a review on crowdfunding and blockchain. Accounting & Finance. Charles Stuart University Melbourne Study Group Centre, Melbourne, VIC, Australia.

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X., Xu, G. 2020. Characterizing cryptocurrency exchange scams. Computers and Security, 98, art. no. 101993, 1-15

Zhang, Y.-J., Bouri, E., Gupta, R. & Ma, S.-J. 2021. Risk spillover between Bitcoin and conventional financial markets: An expectile-based approach. North American Journal of Economics and Finance, 55, art. no. 101296,1-10

Zhou, S. 2021. Exploring the driving forces of the Bitcoin currency exchange rate dynamics: an EGARCH approach. Empirical Economics, 60 (2), 557-606

Zola, F., Bruse, J.L., Eguimendia, M., Galar, M. & Urrutia, R.O. 2019. Bitcoin and cybersecurity: Temporal dissection of blockchain data to unveil changes in entity behavioral patterns. Applied Sciences (Switzerland), 9 (23), art. no. 5003, 1-20

WEB SOURCES

Argo Blockchain 2021. 2020 Annual Report Accounts. (Accessed 2nd December 2021) https://sec.report/otc/financial-report/287335

. Accounting Board 2012. KILA 1895 – Digitaalisen vertaisvaluutan käsittely kirjanpidossa. (Accessed 2nd November 2021)

Bitcoin Group SE 2020. Annual Report 2020. (Accessed 25th November 2021) https://bitcoingroup.com/images/PDF/FB_2020/BitcoinGroup_GB2020_EN.pdf

Deloitte 2021. On the Radar – Fair Value Measurements and Disclosures (Including the Fair Value Option) (Accessed 7th December 2021) https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-fair-value-measurements-and-disclosures-including-the-fair-value-option-April-2021.pdf

FASB 2021. Financial Accounting Standards Advisory Council Meeting Handout. (Accessed 30th October 2021)

https://www.fasb.org/jsp/FASB/Document_C/DocumentPage&cid=1176176260390

FASB 2021. Invitation to Comment – Agenda consultation. (Accessed 30th October 2021) https://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1176176828145

Finnish Customs 2021. Tullin tilinpäätös vuodelta 2020. (Accessed 5th December 2021) https://tulli.fi/documents/2912305/4491356/Tullin%20tilinp%C3%A4%C3%A4t%C3%B6s%20vuodelta%202020/

IAS Plus 2007. IAS 1 – Presentation of Financial Statements. (Accessed 1st November 2021) https://www.iasplus.com/en/standards/ias/ias1

IAS Plus 2011. IFRS 13 – Fair Value Measurement. (Accessed 1st November 2021)

https://www.iasplus.com/en/standards/ifrs/ifrs13

IFRS 2019. Holdings of Cryptocurrencies. (Accessed 30th October 2021)

https://www.ifrs.org/content/dam/ifrs/supporting-implementation/agenda-decisions/holdings-of-cryptocurrencies-june-2019.pdf

International Monetary Fund 2018. Treatment of Crypto Assets in Macroeconomic Statistics. Statistics Department. (Accessed 28th September 2021)

Microstrategy 2020. Form 10-K. https://www.microstrategy.com/content/dam/website-assets/collateral/financial-documents/financial-document-archive/2020-annual-report.pdf (Accessed 19th November 2021)

Mishler, D., M. 2021. A take on cryptoasset transactions, investments, and risks. Journal of accountancy. https://www.journalofaccountancy.com/issues/2021/sep/cryptoasset-transactions-investments-risk.html (Accessed 8th December 2021)

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. (Accessed 3rd November 2021) https://bitcoin.org/bitcoin.pdf

State Treasury 2018. Virtuaalivaluuttojen käsittely kirjanpitoyksikössä. Instruction.

Tesla, Inc. 2021. Form 10-Q. https://ir.tesla.com/_flysystem/s3/sec/000095017021000524/tsla-20210630-gen.pdf (Accessed 22nd November 2021)