POZNAŃ UNIVERSITY OF ECONOMICS AND BUSINESS
Research Papers in Economics and Finance *Vol. 8, No. 2, 2024: 91–104*
https://ref.ue.poznan.pl *https://doi.org/10.18559/ref.2024.2.1868*

Insurability of cryptocurrency wallets

Piotr Manikowski[1] **Weronika Szymczak-Łączna**[2]
Bojan Srbinoski[3]

Abstract

This article concerns the possibilities of insuring cryptocurrency wallets using various assumptions and characteristics of perfectly insurable risk. The main goal of this article is to examine if and how cryptocurrency wallet risk fulfils the requirements of an ideally insurable risk. The research topic is important looking at the latest trends in financial markets and the growing number of cryptocurrency investors. The paper presents the authors' approach to a part of cryptocurrency risk in the insurance industry. The authors analysed the requirements of an insurable risk. They applied these requirements to a specific risk, i.e. the cryptocurrency wallet risk to further check if it is possible to insure such a risk. By introducing and defining cryptocurrency wallet risk, the authors found an element of cryptocurrencies which shows traits of a non-speculative risk and possibly fulfils insurability characteristics.

Keywords

- cryptocurrency
- insurability
- cryptocurrency wallet risk
- ideally insurable risk
- insurance industry

Article received 6 November 2024, accepted 2 December 2024.

Supported by funds granted by the Minister of Science of the Republic of Poland under the "Regional Initiative for Excellence" Programme for the implementation of the project "The Poznań University of Economics and Business for Economy 5.0: Regional Initiative – Global Effects (RIGE)".

Suggested citation: Manikowski, P., Szymczak-Łączna, W., & Srbinoski, B. (2024). Insurability of cryptocurrency wallets. *Research Papers in Economics and Finance*, *8*(2), 91–104. https://doi.org/10.18559/ref.2024.2.1868

[1] Poznań University of Economics and Business, al. Niepodległości 10, 61-875 Poznań, Poland, University St. Kliment Ohridski, Boulevard 1st of May B.B, Bitola 7000, North Macedonia, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah Darul Aman, Malaysia, corresponding author: piotr.manikowski@ue.poznan.pl

[2] Independent researcher, Poland, weronika.szymczak2012@gmail.com

[3] University St. Kliment Ohridski, Boulevard 1st of May B.B, Bitola 7000, North Macedonia, bojan.srbinoski@uklo.edu.mk

Introduction

With the growing dissatisfaction of residents with the actions of governments and central banks, as well as growing fees for monetary institutions' services, there was a growing need of many to create a more borderless, decentralised and digital currency that would keep up with the extremely high development rate of the internet solutions. That is why, in 2009 a developer Satoshi Nakamoto introduced a fully virtual, secured by cryptography, cryptocurrency called Bitcoin. Many years have passed since it all started, and today, the cryptocurrency market capitalisation is estimated to be around 3.5 trillion US dollars, with Bitcoin accounting for more than half of this value (Forbes, 2024). Can such a figure still be ignored by the modern world? Neither the European Union nor a single country has developed any way to approach this novelty from a governmental, institutional and legal point of view.

The topic of this paper concerns the possibilities of insuring cryptocurrency wallets using standard assumptions and characteristics of perfectly insurable risk. The topic is significant looking at the latest trends in financial markets. The ultimate aim of undertaken research is to develop a way to insure a part of cryptocurrency risk which concerns cryptocurrency wallets. However, first, we need to check if that risk is insurable. Thus, the purpose of this paper is to examine how well the risk associated with cryptocurrency wallets meets the criteria for an ideally insurable risk. This study offers a pioneering analysis of the potential for insuring cryptocurrency wallet risk and contributes to the existing literature by evaluating whether this risk fulfils the necessary insurability requirements. The intention of this paper is to encourage further discussion on this topic.

The paper is structured as follows. First, it provides a brief overview of cryptocurrencies along with the relevant legal context in the literature review section. Next, it defines cryptocurrency risk and outlines the fundamental characteristics of cryptocurrency wallet risk. Finally, the authors discuss the requirements of an ideally insurable risk and apply these requirements to a specific risk, i.e. cryptocurrency wallet risk.

1. Literature review

Cryptocurrency is a set of binary data developed to be a medium of exchange, using cryptography. The currency is stored in a database, which secures transaction details, overlooks the creation of new coins and checks ownership rights

(Greenberg, 2011). It is also worth mentioning in this context two important terms that should be distinguished: an "object", which is an asset that can be exchanged, and a "process", which is a technique to transfer the asset to the new user (Lee & Martin, 2020). In the light of the above definition, cryptocurrency, as an "object", has characteristics similar to the national currency since it is exchangeable, it has a set value and online form. It is not new, as there are currencies like the euro or dollar that have the same properties. The extraordinary thing about cryptocurrencies is the "process", since the exchange is fully digital, independent from any third party and decentralised. The mechanism of currency creation and running is purely independent and decentralised, which means that it is not ruled by any government or third party like a central bank. The first decentralised cryptocurrency emerged with the creation of Bitcoin, initially developed by a person or group of people working under the cryptonym Satoshi Nakamoto to be used as a payment system (Skwarek, 2023). However, cryptocurrencies are also treated as an alternative currency, a store of value (Polasik et al., 2015), or a speculative investment (Hileman & Rauchs, 2017, p. 24). Exchanged through blockchain (see wider: Islam et al., 2021, 2022; Rosic, 2018), cryptocurrencies are highly volatile compared to world fiat currencies. As they are not backed by any commodity, basic supply and demand laws do not hold, and the value depends massively on the overall trust of users in this ledger technology (Ilter, 2022).

At the beginning of existence, there were some articles promoting cryptocurrencies. According to Greenberg (2011), Bitcoins have the potential to fully replace state-backed currencies with a digital alternative that is more difficult to counterfeit, transcends international borders, can be stored on personal hard drives rather than in banks, and is not vulnerable to inflation driven by the decisions of Federal Reserve officials to print more money. Taking the perspective of Bitcoin users, we have a fully digital coin that seems to be secure, independent from any country's fiscal or monetary policy and perhaps even resistant to economic fluctuations. This raises the question of why, then, Bitcoin has not become more popular than traditional national currencies. Theoretically, we could use cryptocurrencies to pay for groceries or housing, since it is accepted in payments for goods or services. However, the main obstacle is the fluctuation of value, which influences the purchasing power of cryptocurrency. Based on this we should identify factors which can impact Bitcoin price. The economic literature suggests the following factors: macroeconomic and financial sources, technical contributors as well as speculation (Balcilar et al., 2017; Bouoiyour & Selmi, 2015; Ciaian et al., 2016; Dyhrberg, 2016; Greenberg, 2011; Urquhart, 2018). The first factor is supported by Greenberg (2011) who suspects that Bitcoin price is related to the availability of limited resources and with the increase of mined Bitcoins their price will rise. This approach is followed by Bouoiyour and Selmi (2015) and Balcilar et al. (2017) by adding that the price is highly dependent on an interaction between demand

and supply on the market as well as mined volumes. A key underlying factor here is the predetermined maximum supply of 21 million Bitcoins, which imposes a structural constraint on market dynamics. Ciaian et al. (2016) suggest that the cryptocurrency market exhibits similarities in behaviour to the equity market, implying that Bitcoin prices may show correlations with equity indices and oil prices. Meanwhile, Dyhrberg (2016) argues that cryptocurrencies possess hybrid characteristics, combining traits of both equity and commodity (technical contributors factor). The final factor, speculation, is supported by Bouoiyour and Selmi (2015), as well as Urquhart (2018), who claim that the value of Bitcoin is also very volatile due to the noise of traders and speculators and the so-called market attention. However, we can also take a more psychological approach shown by Luther and White (2014), who suggest that it depends on the eagerness of speculators to hold Bitcoin as an asset, and the willingness of transactors to hold Bitcoin as a medium of exchange.

After the success of Bitcoin through tremendous price appreciation, many investors wanted to invest in the crypto ecosystem. Anyfantaki et al. (2021) proved that the optimal portfolio based on such indexes as the S&P 500 or the Russell 2000 could give in the period 2016–2020 very small returns compared to a portfolio augmented with cryptocurrencies, which gets up to even 200% returns, but because of its volatility, the higher risk connected with owning cryptocurrencies in investor's portfolio exists. Researchers have found that investing in Bitcoins can be treated as a diversification plan since it is not correlated with other investments and can act as a counterbalance for economic risk and market fluctuations in stocks and commodities (Akhtaruzzaman et al., 2019; Anyfantaki et al., 2021; Bakry et al., 2021; Baur et al., 2018; Bouri et al., 2017). However, Bakry et al. (2021) warned that the cryptocurrency risk is far more visible than in any known portfolio of shares, commodities or currencies. There is a massive outflow of investors from riskier portfolio elements like cryptocurrencies. This trend is mainly correlated with recession looms and soaring inflation as well as rising living costs; all in all, regular private investors have less to invest in anything and even more so in cryptocurrencies (BBC, 2022).

Having a basic knowledge of cryptocurrency structure, mechanisms and prospects we can now analyse their legal aspect. Cryptocurrencies in most countries have become a popular online exchange, alongside fiat money. They are slowly becoming a part of the market economy, changing the international legal system to cover this novelty. It seems quite necessary to define the nature of cryptocurrencies, and their legal status and functions to allow the development of regulations in that field. Cryptocurrencies are legal in almost all countries; in simple terms, it is not prohibited to pay using cryptocurrencies.

Since the digital money market has developed and the first cryptocurrency emerged in 2010, in 2018 the European Parliament placed a directive that pro-

vided the first clear definition of virtual currencies as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically" (Directive, 2018). Additionally, this Directive introduced a definition of custodian wallet provider, who is "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies". We can see that it is a clear indication that the legal side of the industry is being developed; now we have not only virtual money but also service-connected with the maintenance of the currency. It is also worth adding that there is a visible trend of extending money laundering and terrorism financing laws with the increase in the popularity of cryptocurrencies. In addition, all providers of services in the virtual money industry are obliged to "identify any suspicious activity" and they should allow the authorities to be able to monitor the use of such currencies according to the Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations. Additionally, the EU wants to ensure that all exchanges for virtual money are registered. (Directive, 2018, Article 47, paragraph 1). As there is a real danger of money laundering, the system seems unsafe. The European Union has not yet specified the aspect of taxation of virtual money, so the regulations are now created only at the country level, but it is a popular phenomenon to develop laws regarding cryptocurrency together with taxation issues for this kind of investment. The taxation of cryptocurrencies varies based on their classification in a given country. If recognized as a commodity, they are taxed under goods and services tax; if classified as electronic money, they are subject to capital gains tax.

2. Methodology

In this part, we examine the risks associated with cryptocurrencies and cryptocurrency wallets. Finally, features of an ideally insurable risk will be introduced. That gives us a basis to examine in the result and discussion section if cryptocurrency wallet risk meets all these criteria.

First and foremost, it is essential to define cryptocurrency risk (abbreviated as crypto risk). Crypto risk refers to the potential loss faced by an individual, characterised by breaches in confidentiality, integrity or control over data, private keys to a crypto wallet or cryptocurrency assets. An increase in crypto risk can erode user trust and diminish the value of their portfolio. The main traits connected with crypto risk include:

- criminal activity, which occurs when our IT system or crypto wallet is invaded,
- confidentiality loss, which can happen once our data is exposed to the general public,
- integrity loss, which refers to the disconnection of our PC or crypto wallet from the general system which provides security,
- control loss, which occurs when a user is unable to access, log into or change anything on their computer or wallet due to a hacker taking control over it,
- data loss, which involves the disappearance of stored data following an attack,
- value loss, which is connected with losing valuable data from our PC or having our cryptocurrencies sent to the hacker's wallet.

The crypto risk is related to personal users. Due to the characteristics of this risk shown above, two types of risk can be introduced: market risk and wallet risk. For this paper, we will use cryptocurrency market risk and cryptocurrency wallet risk to distinguish between those two sets of risks. Cryptocurrency market risk is connected with:

- a criminal activity, which includes actions such as money laundering, black market transactions, or financing terrorism through the misuse of cryptocurrencies,
- the erosion of users' trust, which refers to the decline in confidence in the security and profitability of the crypto market,
- value loss, which refers to significant value fluctuations and instability in the cryptocurrency market.

Cryptocurrency wallet risk involves:

- confidentiality loss, such as wallet hacking, which makes private keys visible to the hacker,
- integrity loss, including changes to the configuration or destruction of the cryptocurrency wallet,
- control loss, such as changes to the password or access key that prevent the rightful user from accessing the wallet,
- data loss, such as the physical loss of content of the crypto wallet or loss of the private key.

It is obvious that cryptocurrencies are extremely volatile, so any type of market protection and hedging is difficult. On the other hand, wallet risk invented and defined for this paper is a part of the crypto risk that has the potential to be secured or even insured by individual users. One can treat access to a crypto wallet similarly to having the key to their car, as both grant control and ownership – without it, access is restricted, and the asset becomes inaccessible. While we cannot insure ourselves against a vehicle's value change, we can still insure it against theft, accident or third party liability. In the same sense we can think of

our crypto wallet – we can have it stolen by a hacker who steals our access credentials or the wallet itself, when it is a hard wallet. Additionally, we can have an accident related to losing our transferred coins due to the wrong key provided, or other unforeseen errors.

Cryptocurrency wallet risk seems to be, partially, similar to cyber risk, against which insurance is already provided on the market. Biener et al. (2015), Eling and Wirfs (2016) and Strupczewski (2017) discuss the insurability of cyber risk. In brief, they found some problems with meeting all criteria of insurability, yet they confirmed the insurability of cyber risk.

Based on this, we are going to examine whether cryptocurrency wallet risk can also be insurable. While many may think there is nothing to insure in this industry, an insurability analysis can be a valuable starting point for developing insurance products since the blooming market of cryptocurrencies is not yet well-explored by the insurance industry.

Rejda at al. (2022, pp. 45–47), along with Berliner (1985, p. 325), who introduced nine features of insurability (which are quite similar), as well as Vaughan and Vaughan (2008, pp. 42–44), proposed several characteristics of an ideally insurable risk:

- there must be a large number of exposure units,
- the loss must be accidental and unintentional,
- the loss must be determinable and measurable,
- the loss should not be catastrophic,
- the chance of loss must be calculable,
- the premium must be economically feasible.

3. Results and discussion

This section discusses if and how the above insurability criteria are met in cryptocurrency wallet risk. First, we have a large number of exposure units, which means that we need to have a large number of items of a similar kind which are prone to the same perils. This requirement is important since it provides the fundament of the law of large numbers, which enables the insurer to collect loss data over time, increase the accuracy of loss prediction and, most importantly, spread the loss of one over the whole group of insured during underwriting (Rejda et al., 2022, pp. 45–46). In our case, there would be several people willing to insure their wallets, particularly as medium to large companies increasingly need to secure their systems with such services due to the increasing number of cyber incidents year

after year. Crypto wallet risk also has the potential to have many exposure units, since the number of cryptocurrency investors rises, and each needs a crypto wallet to manage their keys. Therefore, insurance of certain wallet kinds would surely find its buyers, and possible collaborations with crypto-exchanges could make it a possible add-in while creating the wallet, giving the insurer a large number of users and popularity.

Secondly, the loss must be accidental and unintentional, which means it is unforeseen and purely random for the law of large numbers to apply. Crypto wallet risks are purely accidental and beyond the user's control, as they involve external criminal actors attempting to breach corporate systems or steal wallet credentials. The challenge with cryptocurrencies lies in their decentralised nature and the underdeveloped legal framework. This can make it difficult to report crimes to the police and provide sufficient proof for insurers, complicating the process of filing claims.

The third requirement which states that the loss must be measurable and determinable indicates that the loss should have a clearly defined cause, time, place and amount to allow the insurer to assess whether the loss is coverable under the policy and determine the appropriate payout for the insured. For the crypto wallet risk, we can often define the cause of the loss, such as a lost USB stick containing a hard wallet or a hacked cloud in the case of an online wallet. We can also identify the time and place of the incident, for example, on Monday, 19th of March 2022, on Coinbase. However, determining the exact amount of the loss can be more challenging due to fluctuating cryptocurrency values and the difficulty of tracking all assets within a wallet. However, underwriters can cope with volatility risk by indicating that the compensation (loss coverage) cannot exceed, for example, 125% of the portfolio value at the time the insurance is accepted. This ensures that the coverage is based on the portfolio's value on the specific day it was insured, mitigating the impact of market fluctuations.

The fourth requirement is that the loss should not be catastrophic. This means that while the number of users of insurance should be high, the number of losses should be low, since the pooling of losses is the essence of insurance and provides profits to the insuring company. In the case of crypto wallet risk, we need to have some reinsurance in place, since there is a possibility of massive hacking of crypto-exchange-linked wallets or online wallets provided by a particular cloud.

The fifth requirement is that the chance of loss must be calculable, which means that it needs to be possible to calculate the average frequency and severity of future losses with the accuracy required by the insurer. The ultimate goal is to calculate the premium that will cover the costs and yield a profit for the insuring company. In crypto risk, the frequency can be understood as the number of wallets of a particular kind stolen compared to all wallets held, or the num-

ber of private keys exposed compared to the number of keys generated. It is, however, harder to estimate the severity of loss, since it is a true or false statement – either the wallet key was stolen, or it was not. To determine the wallet value, we would need to evaluate the cryptocurrencies linked to the wallet and owned by us. Thus, the severity of graduation is a challenge for an insurer. The problem here lies in the valuation of cryptocurrencies, given their high volatility. If the insurer bases the severity measurement on the current market value of the lost wallet's cryptocurrency, the insurer assumes the same volatility risk as the cryptocurrency owner. A lost wallet would mean that the insurer compensates based on the market price at the time of the loss, which could significantly differ from the cryptocurrency's intrinsic or real value, leading to potential discrepancies in compensation. That is a speculative risk which no underwriter should accept. Similarly, providing compensation in cryptocurrency does not resolve the issue, as the volatility in its prices still persists. The insurer would still face the same risk, with the value of the compensation fluctuating according to the market price of the cryptocurrency at the time of payout. However, underwriters can manage volatility risk by specifying that compensation (loss coverage) will not exceed, for example, 100% or 125% of the portfolio value at the time the insurance is accepted, in the event of price increases. Alternatively, in case of a price decrease, the wallet value could be indemnified based on the current market price at the time of the incident. Insurers can also set the maximum value of indemnification, similar to cyber risk policies, where coverage typically covers only a small maximum loss (Eling & Wirfs, 2016, p. 26). In this case, the policy would cover a portion of the real portfolio value, allowing the insured to recover some of their portfolio's value in the event of a lost wallet.

The sixth and last requirement is an economically feasible premium, which means that the premium must make the insurance an attractive offer compared to the possible loss. It is indicated that the chance of loss should be less than 40% for the insurer to propose an economically feasible premium (Mehr & Cammack, 1976). In the case of cyber risk, the premium varies depending on the size of the systems and the corporation's tailored insurance offer. However, since companies decide to buy insurance, we can assume that the premium is economically feasible; otherwise, they would think of another possibility to reduce the cyber risk. We can check the cryptocurrency wallet risk by calculating the ratio of the value of stolen crypto wallets to the global market capitalisation of cryptocurrency wallets. As of February 2022, criminal wallets store over $25 billion worth of cryptocurrencies compared to $1.98 trillion of the global cryptocurrency market capitalisation (Hollerith, 2022), thus the chance of loss is as low as 1.26%.

$$\text{Chance of loss} = \frac{\$25}{\$1980} = 0.0126 = 1.26\%$$

We can argue that, even if the chance of loss is close to 40%, it may still seem low enough for some individual users to believe it is unlikely to happen to their wallets. The market for purchasing insurance can be stimulated by offering an economically feasible premium, increasing awareness through the dissemination of information about criminal cases of wallet hacks, as well as raising user awareness based on the type of wallet they use. All in all, we can say that crypto wallet risk complies with all requirements at least partly. Some of the criteria appear to be fully met, while others are met to a limited extent, as illustrated in Table 1.

Table 1. Cryptocurrency wallet risk as an insurable risk

Requirements	Cryptocurrency wallet risk compliance
A large number of exposure units	yes
Accidental and unintentional loss	yes, proof needed
Determinable and measurable loss	partially yes
No catastrophic loss	yes, reinsurance against crypto exchange wallets
Calculable chance of loss	partially yes, a method to determine the severity needed
Economically feasible premium	yes

Source: own research.

As may be seen, the biggest challenge seems to be the valuation of the real value of a portfolio held in a wallet, given the high volatility of cryptocurrencies. Additionally, the value of this asset is influenced by various factors such as market price, investor interest and the amount of currency mined. It looks quite similar to the results of the insurability tests for cyber risk. Eling and Wirfs (2016, pp. 25–26) identified three most problematic aspects of insurability of cyber risks: the randomness of loss occurrence, information asymmetry and the threat of adverse selection, as well as difficulties in measuring losses. However, these authors followed Berliner's (1985) nine-features concept of the insurability of risks.

While many may believe this type of risk cannot be insured, there are ways to provide coverage, even though it is not a perfectly insurable risk. Providers can develop estimation models and incorporate such insurance into their offerings. Therefore, based on meeting the insurability requirements, we can expect the possibility of creating such an insurance product to be quite high. In 2022, such insurance was not available; however, later the first solutions began to emerge, marking the beginning of insurance products tailored to cover cryptocurrency wallet risks.

Thus, at the final stage of this research, we examined the current state of cryptocurrency insurance on the market. Coverage for virtual assets lost or stolen under specific circumstances has become available. However, cryptocurrency insurance providers typically offer these services primarily to institutions such as exchanges,

rather than individual users. Customers can count on compensation only if they are affected by a company's hardware, software or service failures. For instance, compensation may only be available if the exchange where a user stores their private keys is hacked and loses all funds, provided the exchange has insurance coverage for such an occurrence. However, if an individual uses a wallet that the exchange supports but did not create or maintain to store their private keys, they may be out of luck. In such cases, the exchange's insurance may not cover losses, leaving the individual without compensation. Furthermore, no policy protects consumers holding their private keys themselves (Lodge, 2024).

The insurance industry is making some progress. Companies such as Canopius and Evertas have studied the cryptocurrency industry and started offering more relevant insurance for businesses involved in this area. They provide tailored coverage options to meet the evolving needs of their clients, offering a range of policies for different types of wallets. The coverage can include mining hardware and plants against physical loss or damage to mining hardware, as well as theft, loss or damage to both digital and physical assets. This coverage applies to incidents caused by external threats, such as cyber-attacks and criminal activities, as well as risks from insiders (fidelity) (Canopius, n.d.; Evertas, n.d.).

However, insurance for retail cryptocurrency users and investors is still lacking. Some exchanges, like Gemini (n.d.), maintain commercial crime insurance to cover breaches or failures of their systems or applications. Some companies offer plans that cover lost or stolen crypto if the keys are held in a custodial wallet, such as an exchange's cold wallet. However, there are very few, if any, insurance providers offering coverage for crypto users who store their keys themselves or use third-party wallets (Lodge, 2024).

Conclusions

The paper considers the possibility of cryptocurrency wallet risk insurance. It examines if and how well cryptocurrency wallet risk fulfils the requirements of an ideally insurable risk. The aim of the work has been fulfilled and the main problem of the insurability of cryptocurrency wallet risk has been covered. The characteristics of cryptocurrencies presented in the first part led to the conclusion that cryptocurrencies are highly speculative and volatile, thus it is hard to evaluate their intrinsic value, as well as omit financial bubbles around this industry. In the second part, the authors have introduced and defined terms of cryptocurrency risk, cryptocurrency wallet risk and features of insurability. Finally, cryptocurrency wallet risk has been discussed as an insurable risk.

The authors confirm the possibility of insuring this type of risk. The research has eventually led to formulating the following conclusions: cryptocurrencies are too volatile for insurers to take on the risk of covering lost coins. However, other elements of cryptocurrency wallets show, at least partially, the traits of a perfectly insurable risk, which makes it possible to create broker professional insurance extension for crypto wallets. Such insurance can cover basic liability, business interruption and attack mitigation risks, serving as a safety net for financial businesses in the cryptocurrency sector.

Future research in that area could involve comparing crypto wallet risk with similar types of risk, such as cyber risk, for which insurance offers already exist. Based on this, we can consider whether the perils associated with both types of risk are similar or not. That could be a way to develop a proposition or design for a specific insurance cover tailored to crypto wallets.

References

Akhtaruzzaman, M., Sensoy, A., & Corbet, S. (2019). The influence of Bitcoin on portfolio diversification and design. *Finance Research Letters*, *37*, 101344. https://doi.org/10.1016/j.frl.2019.101344

Anyfantaki, S., Arvanitis, S., & Topaloglou, N. (2021). Diversification benefits in the cryptocurrency market under mild explosivity. *European Journal of Operational Research*, *295*(1), 378–393. https://doi.org/10.1016/j.ejor.2021.02.058

Bakry, W., Rashid, A., Al-Mohamad, S., & El-Kanj, N. (2021). Bitcoin and portfolio diversification: A portfolio optimization approach. *Journal of Risk and Financial Management*, *14*(7), 282. https://doi.org/10.3390/jrfm14070282

Balcilar, M., Bouri, E., Gupta, R., & Roubaud, D. (2017). Can volume predict Bitcoin returns and volatility? A quantiles-based approach. *Economic Modelling*, *64*, 74–81. https://doi.org/10.1016/j.econmod.2017.03.019

Baur, D. G., Hong, K., & Lee, A. (2018). Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, *54*, 177–189. https://doi.org/10.1016/j.intfin.2017.12.004

BBC. (2022, June 14). *Bitcoin: Why is the largest cryptocurrency crashing?* BBC News. https://www.bbc.com/news/technology-61796155

Berliner, B. (1985). Large risks and limits of insurability. *The Geneva Papers on Risk and Insurance*, *10*(37), 313–329. https://doi.org/10.1057/gpp.1985.22

Biener, C., Eling, M., & Wirfs, J. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice*, *40*, 131–158. https://doi.org/10.1057/gpp.2014.19

Bouoiyour, J., & Selmi, R. (2015). What does Bitcoin look like? *Annals of Economics and Finance*, *16*(2), 449–492.

Bouri, E., Gupta, R., Tiwari, A., & Roubaud, D. (2017). Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. *Finance Research Letters*, *23*, 87–95. https://doi.org/10.1016/j.frl.2017.02.009

Canopius. (n.d.). *Digital asset insurance*. Retrieved November 4, 2024 from https://www.canopius.com/insurance/cryptocurrency-insurance/

Ciaian, P., Rajcaniova, M., & Kancs, d'Artis. (2016). The economics of BitCoin price formation. *Applied Economics*, *48*(19), 1799–1815. https://doi.org/10.1080/00036846.2015.1109038

Directive. (2018). Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018, p. 43–74).

Dyhrberg, A. (2016). Bitcoin, gold and the dollar – A GARCH volatility analysis*. Finance Research Letters*, *16*, 85–92. https://doi.org/10.1016/j.frl.2015.10.008

Eling, M., & Wirfs, J. H. (2016). *Cyber risk: Too big to insure? Risk transfer options for a mercurial risk class*. University of St. Gallen. https://www.ivw.unisg.ch/de/studie/cyber-risk-too-big-to-insure-risk-transfer-options-for-a-mercurial-risk-class-band-59/

Evertas. (n.d.). *Insurance*. Retrieved November 4, 2024 from https://evertas.com/insurance/#crime-theft-loss

Forbes (2024, November 25). *Cryptocurrency Prices Today By Market Cap*. https://www.forbes.com/digital-assets/crypto-prices/?sh=49d47f6a2478

Gemini. (n.d.). *Cryptoasset Insurance*. Retrieved November 4, 2024 from https://www.gemini.com/legal/gemini-digital-assets#section-cryptoasset-insurance

Greenberg, A. (2011, May 13). Crypto Currency. *Forbes*. https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html

Hileman, G., & Rauchs, M. (2017). *Global cryptocurrency benchmarking study.* Cambridge Centre for Alternative Finance. https://doi.org/10.2139/ssrn.2965436

Hollerith, D. (2022, February 16). *Illicit crypto wallets hold over $25B as hacks, thefts mushroom*. https://finance.yahoo.com/news/data-illicit-crypto-wallets-hold-over-25-b-as-hacks-thefts-mushroom-142721296.html

Ilter C. (2022). How dependable are blockchain and cryptocurrencies? *Journal of Taxation of Investments*, *40*(1), 75–84.

Islam, M., Rahman, M., Rahman, M., Mohamad, M., & Embong, A. (2021). Cryptocurrency integration challenges in blockchain for financial institutions. *Asian Journal of Electrical and Electronic Engineering*, *1*(2), 28–36. https://doi.org/10.69955/ajoeee.2021.v1i2.18

Islam, M., Rashid, M., Rahman, M., Mohamad, M., & Embong, A. (2022). Analysis of blockchain-based Ripple and SWIFT. *Asian Journal of Electrical and Electronic Engineering*, *2*(1), 1–8. https://doi.org/10.69955/ajoeee.2022.v2i1.26

Lee, M., & Martin, A. (2020, June 18). *Bitcoin is not a new type of money*. Federal Reserve Bank of New York Liberty Street Economic. https://libertystreeteconomics.newyorkfed.org/2020/06/bitcoin-is-not-a-new-type-of-money/

Lodge, M. (2024, August 24). What is crypto insurance? *Investopedia*. https://www.investopedia.com/crypto-insurance-5441920

Luther, W., & White, L. (2014, June 5). *Can Bitcoin become a major currency?* GMU Working Paper in Economics, No. 14–17. https://doi.org/10.2139/ssrn.2446604

Mehr, R., & Cammack, E. (1976). *Fundamentals of insurance*. R.D. Irwin.

Polasik, M., Piotrowska, A., Wisniewski, T., Kotkowski, R., & Lightfoot, G. (2015). Price fluctuations and the use of Bitcoin: An empirical inquiry. *International Journal of Electronic Commerce*, *20*(1), 9–49. https://doi.org/10.1080/10864415.2016.1061413

Rejda, G., McNamara, M., & Rabel, W. (2022). *Principles of risk management and insurance* (14th ed.). Pearson

Rosic, A. (2018, April 9). *What is blockchain technology? A step-by-step guide for beginners*. https://www.ieyenews.com/what-is-blockchain-technology-a-step-by-step-guide-for-beginners/

Skwarek, M. (2023). Is Bitcoin an emerging market? A market efficiency perspective. *Central European Economic Journal*, *10*(57), 219–236. https://doi.org/10.2478/ceej-2023-0013

Strupczewski, G. (2017). The cyber-insurance market in Poland and determinants of its development from the insurance broker's perspective. *Economics and Business Review*, *3*(2), 33–50. https://doi.org/10.18559/ebr.2017.2.3

Urquhart, A. (2018). What causes the attention of Bitcoin? *Economics Letters*, *166*, 40–44. https://doi.org/10.1016/j.econlet.2018.02.017

Vaughan, E. J., & Vaughan, T. M. (2008). *Fundamentals of Risk and Insurance* (10th ed.). John Wiley & Sons, Inc.