Journal of
Risk and Financial Management

MDPI

Review

A Cryptocurrency Spectrum Short Analysis

Mircea Constantin Șcheau [1], Simona Liliana Crăciunescu [2], Iulia Brici [3] and Monica Violeta Achim [3,*]

[1] Faculty of Automation, Computers and Electronics, University of Craiova, 200585 Craiova, Romania; mircea.scheau@edu.ucv.ro
[2] Simona Liliana Crăciunescu, The Bucharest University of Economic Studies, 010374 Bucharest, Romania; liliana.craciunescu@gmail.com
[3] Faculty of Economics and Business Administration, Babeș-Bolyai University, 400591 Cluj-Napoca, Romania; iulia.brici@econ.ubbcluj.ro
* Correspondence: monica.achim@econ.ubbcluj.ro

Received: 30 June 2020; Accepted: 11 August 2020; Published: 17 August 2020

Abstract: Technological development brings about economic changes that affect most citizens, both in developed and undeveloped countries. The implementation of blockchain technologies that bring cryptocurrencies into the economy and everyday life also induce risks. Authorities are continuously concerned about ensuring balance, which is, among other things, a prudent attitude. Achieving this goal sometimes requires the development of standards and regulations applicable at the national or global level. This paper attempts to dive deeper into the worldwide operations, related to cryptocurrencies, as part of a general phenomenon, and also expose some of the intersections with cybercrime. Without impeding creativity, implementing suggested proposals must comply with the rules in effect and provide sufficient flexibility for adapting and integrating them. Different segments need to align or reposition, as alteration is only allowed in a positive way. Adopting cryptocurrency decisions should be unitary, based on standard policies.

Keywords: cryptocurrencies; fraud; algorithms; correlations; impact; risks; regulation; blockchain

1. Introduction

In the area of influence of computer science, the terms undergo rapid mutations, both in sense and interpretability. Even if some have ephemeral appearances, those supported by well-defined reasons are assimilated and reclassified or regrouped, their similarities widening the spectrum of understanding the phenomenon.

According to a study by Data Bridge Market Research based on data from 2015 to date, without considering an a priori order, the top 10 cloud technologies that dynamically divide most of their market shares refer to Hybrid Cloud, Cloud Storage, Cloud Migration Services, Cloud Orchestration, Platform-As-A-Service, Disaster Recovery-As-A-Service, Multi-Cloud Management, Video-As-A-Service, Cloud Analytics, and Wi-Fi-As-A-Service. We do not estimate that the debate regarding the benefits and vulnerabilities introduced by modern storage and processing facilities, compared to traditional structures, will stop at any time soon. Perhaps a mixed architecture is a valid compromise until a new viable alternative emerges. Until then, we can only monitor adoption and note that financial organizations are more focused on saving and processing information in the cloud (96%), according to cybersecurity expert Ryan Brooks. In some instances (34%), there was a declarative improvement in the IT infrastructure security, while for others it worsened (22%) or reported no change (31%). Overall, 88% agreed to transfer sensitive data to the cloud, while 47% advocated a cloud-first approach.

These references can be correlated with those reported by Dan Williams, senior cybersecurity systems engineer, regarding ransomware. His 2017 statistics indicated a total of 9.2 billion global attacks, a 101% increase in the number of developed variants; only 42% of companies managed to restore their databases using backups, and Petya was the most common malicious product during an email campaign.

We estimate that the connection between cloud, cyber-crime, and cryptocurrency is getting stronger, and the distributed consequences are directly proportional to the evolution graph of each one. Analog and inductive research methods are very well suited to the subject, and we believe that the reason–effect ratio and adjustable inflection points can be expressed with sufficient clarity by changing the parameters.

Cryptocurrencies feature both benefits and disadvantages. The subtle way in which they appear is the main reason why they have made changes in the financial market. This is where the most significant threats come from, specifically cybercriminal activities that are becoming easier to carry out. Additionally, blockchain technology can produce changes in various fields of activity, as long as there is no superior technology to challenge it. For this reason, careful study of cryptocurrency issues is an essential step in both economics and research.

The purpose of this research is to explain what cryptocurrency is, how important it is, how it has evolved, what its use brings to the economy, and what influence cryptocurrency has on cybercrime. This paper focuses more on the arguments, connections, implications, risks, algorithms, regulation, and standardization, and less on the technical aspects of blockchain, block of blocks, or multichain.

Deliberations on the advantages and disadvantages in this direction have been made and will probably continue to be the subject of other specialized studies for a long time. We can say that an optimum is identified if it responds positively to the evaluation criteria.

2. Literature Review

To define cryptocurrency and its role, conceptual aspects related to virtual currencies are available in the literature review section.

Cryptocurrency emerged around 2014 along with the FinTech concept, and it is now a part of the larger digitalization process. Up to 2018, the literature has revolved around the concept of cyptocurrency and diversified classification. However, post-2018, authors have chosen fascinating niches of the literature.

In 2019, Corbet et al. (2019) mentioned cryptocurrencies as a financial asset. The paper presented a review of the literature from an empirical point of view of the aspects associated with cryptocurrency as a financial asset, since its appearance. Based on previous papers, the author chose the topic of cryptocurrency because of existing questions about market efficiency, asset pricing bubbles, contagion, and decoupling hypotheses or volatility clustering. Situated at the intersection between regulatory oversight, the potential for illicit use through its anonymity within a young under-developed exchange system and infrastructural breaches influenced by the growth of cyber criminality, the role of cryptocurrency proves to be influenced by each of these. Furthermore, in 2019, Bouri et al. (2019) studied the similar movements of cryptocurrencies. They set Bitcoin as the reference currency and discovered the presence of concurrent movements, in the same direction, of 12 types of cryptocurrencies. As a basis for research, they used daily data on the price of cryptocurrencies. The study found that the movement of one cryptocurrency determines, in a large proportion, the movement of other cryptocurrencies in the same direction. The process is called co-jumping. The study concluded that their trading volume highlighted the volatility of cryptocurrencies.

In 2019, Chu et al. (2019) investigated the adaptive market hypothesis regarding the markets of two popular cryptocurrencies (Bitcoin and Ethereum) against the Euro and the U.S. dollar where the results were consistent with this theory. The authors also discussed that events could coincide with significant changes in market efficiency. The sentiment of these market efficiency factors was verified using a simple analysis of events to investigate whether these actions affected market

efficiency/inefficiency. The bottom line is that sentiment and events cannot be a significant factor in determining the effectiveness of cryptocurrency markets. The collected data involved logged hours with high-frequency Bitcoin and Ethereum prices against the Euro (EUR) and the U.S. dollar (USD). It followed transactions listed on the Kraken cryptocurrency exchange starting 11:00 a.m. on 1 July 2017 until 12 a.m. on 1 September 2018. The particular timespan was selected so that we could analyze the intervals in which prices for the two cryptocurrencies faced huge spikes (before January 2018) and slumps (after January 2018). The results appeared to be consistent with the hypothesis, where the efficiency of the markets varied over time.

In 2018, Zhang et al. (2018) also wrote about the 'stylized facts.' Cryptocurrencies were investigated as a financial asset. They analyzed the stylized facts in terms of the Hurst exponent by using the Detrended Fluctuation Analysis (DFA) and R/S Analysis, of the four most popular cryptocurrencies ranked according to their market capitalization. The datasets contained historical high-frequency prices of those cryptocurrencies versus the U.S. dollar, from 25 February until 17 August 2017. The top four chosen cryptocurrencies for our analysis involved Bitcoin, Ethereum, Ripple, and Litecoin. The study was conducted on high-frequency returns data with varying lags. It also considered features of dependence between the different cryptocurrencies. These features provide academics and industrial practitioners with information about the structure and characteristics of these four popular cryptocurrencies and may also be useful in developing models of pricing cryptocurrencies.

Other authors such as Xu et al. (2019) have measured the tail-risk interdependence between 23 cryptocurrencies using previous methods. They estimated the value at risk (VaR) for each cryptocurrency by using quantile regression, also called the Tail-Event driven NETwork (TENET) framework. With the help of this study, it was identified that a significant risk spillover effect exists and that the degree of the total connectedness of all the sampled cryptocurrencies increased steadily over time. Bitcoin seems to be the most significant systemic risk receiver, and Ethereum the largest systemic risk emitter. Like Bouri did, Grobys also developed a study in (Grobys et al. 2019) based on the daily data of the price of cryptocurrencies. This time, their processing involved determining the moving average trading strategies employ. The 11 most traded currencies from 2016–2018 were used for this purpose. The result indicated that a variable moving average strategy is successful when using a 20-day moving average trading strategy. In addition, the results revealed that cryptocurrency markets were inefficient. Another study by Corbet et al. (2020) showed the destabilizing effects of cryptocurrency and cyber criminality. The purpose of the article was to discover what the financial market effects of recent cybercrime were in cryptocurrency markets. Corbet used data from the Bitfinex exchange at a 60-min frequency for the eight most liquid cryptocurrencies. The results led to the conclusion that hacking events also increased both the price volatility of the targeted cryptocurrency and cross-cryptocurrency correlations. Cybercrime events reduce the price discovery sourced within the hacked currency relative to other cryptocurrencies. In 2019, Koerhuis et al. (2019) conducted a forensic analysis of privacy-oriented cryptocurrencies and found that criminals used cryptocurrencies that had built-in anonymity and privacy features that made them nearly impossible to trace funds back to a particular user in different kinds of malware to launder money. The author investigated Monero and Verge and studied which valuable forensic artifacts the software of these cryptocurrencies left behind on a computer system. Different sources of potential evidence were also examined in this paper.

In another article, Caporale et al. (2019) wrote about non-linearities, cyber-attacks, and cryptocurrencies. For this purpose, he used a Markov-switching non-linear specification to analyze the effects of cyber-attacks on the returns of four cryptocurrencies from 2015 to 2019. The analysis considered cyber-attacks and targeting cryptocurrencies. The results suggest the existence of the significant adverse effects of cyber-attacks on the probability of cryptocurrencies staying in the low volatility regime. This reveals the importance of knowing how to deal with cybercriminals to prevent the disruptions of the markets.

3. Standardization and Regulations

A report elaborated by The Law Library of Congress, Global Legal Research Center, Staff of Global Legal Research Directorate (2018) examines the legal, political, and fiscal landscape regarding the regulated status (or not) of cryptocurrencies in over 100 countries and notes that the terminology of addressing (and implicitly of perceiving cryptocurrencies) differs from one jurisdiction to another (Figure 1). In Taiwan, China, and Canada, cryptocurrencies are seen and described as a virtual commodity; in Mexico and Honduras as a virtual asset; in Thailand and Argentina as digital currency; in Lebanon and Colombia as electronic currency; in Italy as cyber currency; in Switzerland as token payment; in Germany as a crypto-token, etc. The approach is different and reflects the acceptance decisions (or not) as a means of payment or taxation method. For example, Switzerland taxes cryptocurrencies as foreign currency, while in Israel, they are assets. If some jurisdictions impose direct or indirect restrictions (e.g., by financial restriction) on investments in cryptocurrencies, others prohibit citizens from engaging in activities at the local level, but not abroad.

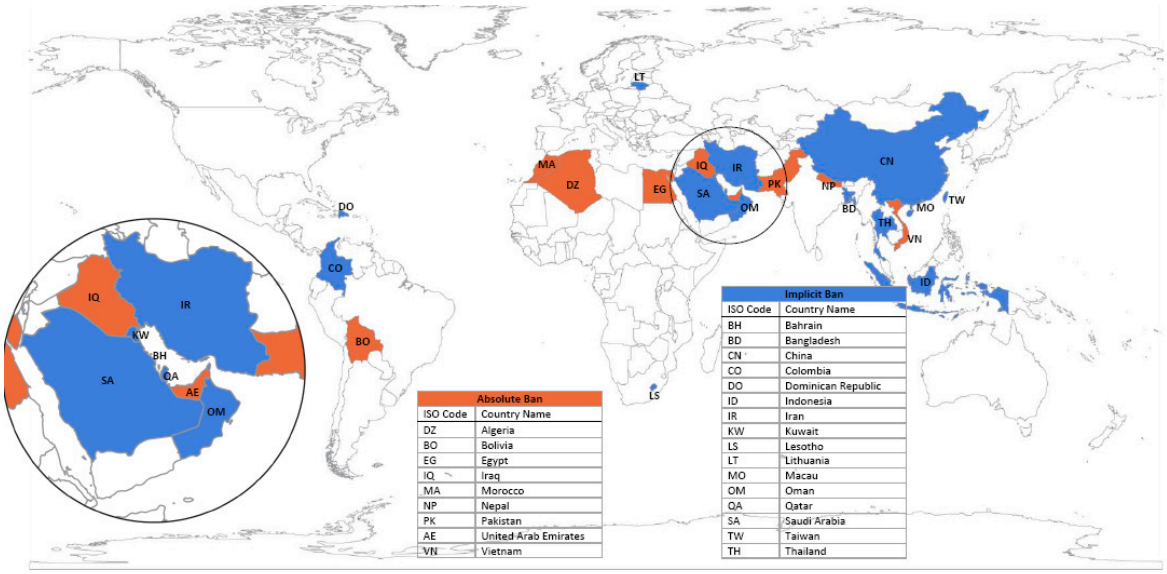

Figure 1. Legal status of cryptocurrencies. Source: Staff of Global Legal Research Directorate (2018).

The European Central Bank and the national central banks may also open accounts for participating credit institutions or public entities according to national regulations for insurance companies or other parties involved in the transaction or transfer process (Zellweger-Gutknecht 2018). One of the challenges generated by the desire to regulate cryptocurrencies brings to the forefront the need to combat money laundering, which is focused on combating terrorism financing while monitoring illegal markets (e.g., drug trafficking, trafficking in human beings, etc.). Another challenge refers to rules concerning securities and consumer and investor protection guidelines. Regulatory boundaries need to take into account concrete realities, in which the delimitation of responsibilities of various authorities from the jurisdiction point of view related to cryptocurrencies is rather unclear. Central banks adopt a prudential policy, capitalizing on digital technologies in the direction of saving resources. Distributed Ledger Technology components apply inter alia to the Central Bank Digital Currency (CBDC) and therefore must be modeled on authorized protocols. The design should include options for reserve convertibility to support day-to-day liquidity, minimizing settlement risks (Bank for International Settlements 2018). In addition, the introduction of the CBDC as a guarantee, deposit facilitation for commercial banks, or the interest payable for individuals' holdings emphasizes fixing margins that are difficult to control. Taxation of profits earned by individuals or intermediary companies implies the existence of "monetary" legislation, tax provisions, and clear enforcement rules. The likelihood of correlation is rather low in terms of end-user anonymity, and it is virtually impossible to comply with the

minimum Know Your Customer/Client (KYC) provisions, which are also necessary for risk assessment. Nevertheless, we are witnessing bold moves regarding the assimilation of Financial Technology and FinTech-blockchain into platforms dedicated to banking operations. The open architecture is designed to be flexible and tailored to the needs of customers, with the digitized models in operation validating the avant-garde character (Erste Group 2018).

A new tendency, which was perhaps born out of the desire to eliminate one of the most disturbing factors, is to freeze values. It theoretically addresses players who do not have a high-risk appetite and who want to trade at default quotes. Anonymity is maintained, but parity is fixed in comparison with a widely-recognized financial standard. Specifically, the cryptocurrency is supported by an equivalent amount in one of the traditional currencies (e.g., dollar, euro, or Japanese yen) and may be deposited in an account. The native tokens trading under the USD symbol in 2014 were about twenty-five million units, with more than 2.5 billion units in circulation by the end of 2018. At the time of issue, a Tether was quoted at the value of one US dollar, and a Roncoin, built on the Ethereum blockchain platform, was rated at the cost of one Romanian RON. Tether allows for dollar-like operations without a bank connection and can be converted into another cryptocurrency, with leverage in manipulating quotes. 'Scheduled' Tether issuing and the acquisition of cryptocurrencies almost always have a strong effect on stabilizing or raising prices, with massive reconversion leading to a controlled decline. Symmetrical or asymmetric correlations were carefully investigated, and the results were delivered in graphical form and tables (Griffin and Shams 2018) as clearly as possible.

In the same context, the idea of creating a decentralized cryptocurrency using blockchain technology, whose parity is in line with the global gold quote, has begun to emerge. More precisely, through the token process, AurusGOLD (AWG) was born. Each currency represents the equivalent of one gram of 99.99% pure gold at the London Bullion Market Association's accepted quotation. The cryptocurrency is claimed by promoters, some of whom have gained experience in specialized software firms in a country located at the intersection of Central, Eastern, and Southeast Europe, that it is designed to support market pullout at any time, supported 100% by physical gold, and that the storage and securing of the precious metal is in line with the international regulations in force including those on the payment of taxes. The debate aims at the direct convertibility of gold–cryptocurrency, under the conditions of a regulatory vacuum in this area and predictability placed under the sign of doubt (BitScreener 2018). Regardless of the asset attempted for anchor, manipulation is present in several forms, with one or more powerful players having the ability to force the platforms. Making seemingly valid operations without real holdings through scheduled robots and exploiting hourly intervals has revealed new market vulnerabilities, which are responsive to false messages and fraudulent transactions. Even though the material treated rigorously, with extensive robustness checks, addresses the Bitcoin ecosystem, the evaluation can easily be extrapolated to the crypto phenomenon generally, or to any other cryptocurrency in particular (Gandal et al. 2018).

In the report submitted for analysis in July 2018 to the G20 (Group of Twenty, International Forum set up in 1999), it was noted that the Financial Stability Board (FSB) has developed, together with the Committee on Payments and Market Infrastructures (CPMI), an identifying metrics frame to monitor transmission channel implications, exposure, growth rate, convertibility, volatility, transparency, accessibility, jurisdiction, and other elements that can influence the financial stability of cryptographic markets. CPMI pays special attention to payment innovations and provides assistance and advice in studying topics related to decentralized assets or support assets. The International Organization of Securities Commissions has developed a support platform for enrolled members to look into possible cross-border issues, investor protection, regulatory matters, etc. The question is whether the line of conduct designed for secondary markets is also pursued in this case, especially if we take into account critical issues related to custody, settlement, cybersecurity, and system integrity. As we have already said, the legal status of cryptocurrencies is quite unclear, and the weather variations in the quotes lead to changing the calculation coefficients. The terminology is somewhat fluid and indicates a focus on property regulation, with crypto-tokens being often equated with securities, instruments used to

raise funds by representing a security or tangible asset, tangible things that can be held, or controlled (e.g., buildings, commodities, patents, etc.). New indicators refer to capital: the minimum required balance of reserves, custody, pledges, receivables, accounting records, private or property rights, transfer rights, assignment, future contracts, solvency, bankruptcy, etc. Are we finally discussing the regulation of goods, money, assets, financial instruments (e.g., promissory notes, checks, securities, etc.) or the regulation of commercial services?

The convertibility on demand of a cryptocurrency as a legal means of payment, the admissibility of cryptocurrencies and related products such as derivatives traded on stock exchanges (Auer and Claessens 2018) is one of the reasons why the Basel Committee on Banking Supervision quantifies direct and indirect exposure, monitors the evolution of FinTech's crypto-assets, and seeks to clarify prudential procedures from banks and supervisors. Respecting all the compliance rules is one of the stated goals, and the implementation of RegTech (Regulatory Technology) solutions aims to increase transparency and consistency, with the correct interpretation of ambiguous regulations, to impose the right level of quality.

Similarly, the Euro Cyber Resilience Board was created, a forum for cooperation between central banks, supervision institutions, and critical financial infrastructure providers, responsible fiscal policies and economic reforms being under discussion. Governance studies occupy an important place in the list of relevant concerns and are added to those dedicated to improving the financial transaction mechanics. Due to their high volatility, the crypto-assets should have an assigned risk weight around the minimum 1000% threshold, the weighting coefficients varying according to the nature of the crypto-asset. The financial market supervisory authorities will express the consensus within the Basel Committee by developing an international standard.

One thing is clear: international collaboration is essential in the successful imposition and enforcement of rules for combating tax evasion, money laundering, and terrorist financing. An initiative on a unified global regulatory framework must be supported by all official organizations involved such as the G20, the Egmont Group, the FATF or the UN Office on Drugs and Crime (Robby and Snyers 2018).

4. Primary Analysis of Cryptocurrencies

This section includes a proper analysis of cryptocurrencies, focusing on the structure, evolution, and volumes of virtual currency transactions.

According to a study made by Jeff Desjardins (2017) for Visual Capitalist, at the starting point of the cryptocurrency era, the total amount of money in the world between 2014 and 2015 was $90.4 trillion and only about 8% of the money was in physical form. Initial Coin Offering (ICO) is regarded as part of a critical topic, closely related to the theme of cryptocurrencies and the blockchain, representing the main fund-raising mechanism for new projects and unique ideas. As we have already said, some can be a real success, and others may prove to be scams. In 2017, these ICOs benefited, based on service offerings or product offerings, from funding over $6.5 billion for about 450 proposals, and in 2018, getting seven billion for just over 1000 projects.

According to the latest information provided by coinhouse.com (8 April 2020), from over 2000!existing types of cryptocurrency, Bitcoin holds the market majority, as can be seen in Figure 2, totaling 64.55%.

In terms of 24 h purchase volume, on May 2020, the ranking was slightly different, with Bitcoin ranking second under Tether with 56.16 trillion U.S. dollars (Figure 3).

According to the data (Figure 4), the vast majority of currencies move in the same direction as Bitcoin, with small variations over the same time frame. We can conclude that the significant events that affect Bitcoin's price, change in value, profitability, or investments also affect the entire market proportionally. To reinforce and also prove what we have already said, we present Figure 4, compiled with Thomson Reuters data, who has kept a record since 2012, way before cryptocurrency was on the rise, up to now (Figure 4). The movements made in almost the same direction were evident by observing the last three years of analysis.

Figure 2. The share of cryptocurrencies in the world market in 2020. Source: coinhouse.com.

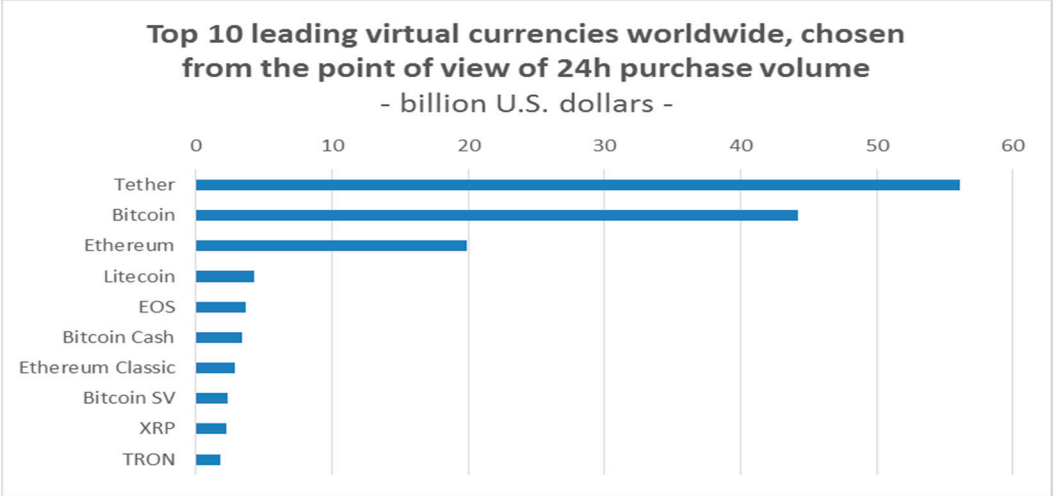

Figure 3. Top 10 leading virtual currencies worldwide. Source: Authors' own processing based on Statista data.

Figure 4. The evolution of worldwide cryptocurrencies, 2012–2020. Source: Authors' own processing based on Thomson Reuters data.

Continuously evolving since its appearance, the price of Bitcoin reached an unprecedented peak in 2017. Then, at the beginning of 2018, more precisely, on January 4, came the phenomenon known as the Great Crypto Crash (Figure 5). For about one month, as a consequence of this event, the price of

Bitcoin fell sharply by about 65%. That moment highlighted, more than ever, that the movements of Bitcoin are followed by the other cryptocurrencies, which reached declines of up to 80%.

Figure 5. The Great Crypto Crash. Source: Authors' own processing based on Thomson Reuters data.

The correlation between the reference cryptocurrency, Bitcoin, and 12 other cryptocurrencies was described in Bouri's study (Bouri et al. 2019), which contained data recorded from 8 August 2015 to 28 February 2019. The highest positive correlation we could see was between the reference cryptocurrency and Litecoin (0.6178), and the weakest was between Bytecoin and Litecoin (0.0697).

5. Influences of Cryptocurrencies on Cybercrime

One of the main characteristics of cryptocurrencies—pseudo-anonymity or total anonymity—can be seen as a bridge to the criminal field, and cybercrime in particular. Haken is a consulting company that audits blockchain systems and more to discover vulnerabilities and fraud with service packages covering a large number of customer needs. Following analysis, a list of essential value frauds related to new or old ICOs is published on the blog, Monero being one of them because it trades in the dark web and uses a type of encryption that theoretically ensures 100% anonymity.

We can highlight Modern Tech, a Vietnamese company that developed an ICO and managed to raise funds for Pincoin of about $660 million from over 32,000 people, and then disappeared from the market. Another example is Plexcoin, which capitalized $15 million, and the administrators were fined by the Securities and Exchange Commission, arrested, and convicted. Building on a good marketing campaign, Benebit has attracted many investors and nearly $3 million.

Established entities abuse the status of "online influencer", DJ Khaled, Floyd Mayweather, and Centratech, who accumulated more than $32 million until discovered. Fifteen people have been arrested in Taiwan for an estimated $8.6 million in fraud, promoting IBCoin, a currency that is strictly usable in adult industries.

Since the beginning of 2019, the legitimacy of two major ICOs—Neluns for $136 million and Ruby-X for $1.2 billion—has been investigated. The EOS project, which raised over $4 billion, pushed the currency into the top 10 most important virtual currencies. EOS is a platform that supports decentralized applications, creating a more friendly environment for developers. CoinDesk statistics, the leading platform for the community of people interested in blockchain and cryptocurrencies) for 2018 indicated that an ICO could raise an average of $25 million, with estimates that 11% of the total amount of money generated by ICOs each year would be scams, with losses amounting to about $250 million in 2018 alone.

Another form of online scam related to cryptocurrencies is promoted in the Defense of the Ancients game (DOTA) players community, the Multiplayer Online Battle Arena video game developed and supported by Valve Corporation. Screensaver files for Windows sent through chats contained scripts that could modify the computer's configuration, record keyboard activities, and, implicitly,

the credentials introduced. This method is also standard in other communities, so it is recommended that more attention is given, especially if the files have the SCR extension.

According to an article made by Kaspersky (2020), other common scams are imposter websites, which seem to look like the original ones. The 's' from 'https' in the link indicates the real website of a company. Another common way of cheating in this area is fake mobile applications. These are available in the App Store, and are difficult to detect. Many people have been victims of cryptocurrency transactions in such counterfeit applications. Usually, there is a misspelling in their name or the representative image of the brand is noticeably modified; very common are scams due to bad tweets or other social media updates. There are many impostors who claim to be well-known people and demand small amounts of money, but who never recover once you become trapped. Perhaps the most common scam are bad emails. We often receive emails from seemingly legitimate companies that want to invest in our digital currency. Through a simple search of the respective company, we can find out if the information is true or only someone trying to fool us, wanting to procure substantial funds from the movements that we allow them.

2019 was a year full of fraud and cybercrime where about $4.26 trillion was stolen from cryptocurrency exchanges. The culprits go unpunished if they attack unsuspecting users. According to an article written in 2020 by Business Insider (2019), among the biggest scams was the exchange between BITPoint and the Japanese cryptocurrency with a resulting loss of 28 million dollars. Bitcoin, XRP, Ethereum, Litecoin, and Bitcoin Cash were stolen in this event.

Another event, which took place in May 2019, was the theft of 40 million dollars through an exchange with Binance. Even if no one expected such an event to take place, Binance could not stop the attack because the hackers who executed this scam were very well organized.

In June 2019, six people suspected of a $27 million Bitcoin scam were arrested. The theft affected more than 4000 victims from 12 different countries. The method used was "typosquatting", which involves creating a fake online cryptocurrency to gain access to victims' Bitcoin wallets.

June also saw hackers obtaining XRP worth about $10 million from GateHub users, and cybercriminals have compromised about 100 Ledger Led wallets.

Bitrue is a cryptocurrency exchange in Singapore that lost $4.2 million in June 2019. Hackers bypassed the exchange's security system, thus exploiting a risk control issue.

Phishing is also present in the world of cryptocurrencies, with at least one clone for each ICO site. There is a need to set up official Internet traffic monitoring structures to remove fraudulent links in browser searches and social networking news as these methods are increasingly taking a toll by exploiting naivety, promising fabulous gains that are just a click away (Khatwani 2018 and PYMNTS 2018).

Two Israeli brothers were arrested after a three-year phishing scam. Meanwhile, the two stole $100 million worth of cryptocurrency by attracting investors such as large companies, imitating cryptocurrency exchanges.

According to a study made by ZD Net (n.d.) in 2020, a total of 109 people involved in the PlusToken cryptocurrency fraud have been arrested in China. This cryptocurrency from South Korea was marketed as a high-yield investment opportunity for traders interested in cryptocurrencies. Investors have allocated funds in Bitcoin, Ethereum, and EOS. As a result of the scam, $3 billion was taken from about four million users. The attack was also through phishing, but this time, chain phishing.

An article written in 2020 by AARP (2020) tells us that, in order not to be the victim of an unfortunate event like the ones above-mentioned, there are a few things to keep in mind. First, it is not appropriate to invest in virtual currencies whose functionality we do not understand. The purchase of virtual coins is not recommended following advice received from anonymous companies by email or advertising. It is also not recommended to invest money from a pension fund in cryptocurrencies. It is imperative to know not to share "private keys" that allow us to access the virtual currency, with anyone.

According to an article written by CoinDesk (2020), a scam can be identified if we know a few tricks. If it is a website we have met before and promises instant returns for small crypto investments, it is definitely a scam.

The first step before using any cryptographic website is to contact a known third party. CoinDesk answers questions about cryptocurrencies and related scams.

Hackers use the image of celebrities to manipulate and fool people. On social networks, the original accounts have a blue check mark next to the name. Other accounts with the same name are held only by imposters.

If we have already sent money to a cryptocurrency wallet, it is probably gone. Scammers can easily withdraw funds by buying and selling cryptocurrency. If the wallet provider is notified, they can sometimes try to stop transfers, but this rarely works.

A very important thing is that anyone who says you can get rich quick only talks about themselves as such a thing cannot be generally true.

"The butterfly effect" leads to an artificial increase in demand, volumes, and premature maturation of the industry. As an example, according to speculation and analysis by market players and unconfirmed by the targeted managers, the financial platform for cryptocurrencies Bitforex became, within a few months of launching, one of the best rated virtual currency exchange platforms with a technique fraudulently known as "wash trading". To unmask the perturbators with uncertain intentions, they compared their online activity, the number of users, the number of unique visitors on the website, the number of social network subscribers combined with the volumes traded by them, reported at the same time in other top 10 markets. Concretely, if the volume traded by a user on the Bittrex trading platform in June 2018 was $280, $861 on the Binance exchange platform, and the BitForex volumes traded by a single user in a month were nearly $13,000, the calculated figures have a source in https://coinmarketcap.com/, specifically the 24 h volume exchanges.

As a specific situation, in Romania, CoinFlux, one of the leaders in exchange services with volumes of over 185 million €, ceased to work as a result of an investigation into its actions carried out in 2018, with banks not allowing transfers to be carried out through bank accounts (e.g., Transilvania Bank, BRD-Groupe Société Générale, etc.). Still, applications such as Revolut or Mistertango can ensure debiting by way of bypassing the electronic wallet, converting the money into virtual currencies. Even if a contradiction with one of the main characteristics of the cryptocurrencies–anonymity—can arise, at the beginning of 2018, the National Agency for Fiscal Administration requested that the earnings from the trading of virtual coins be taxed, this being stipulated in Law no. 30/2019 of 10 January 2019 for the approval of Government Emergency Ordinance no. 25/2018 regarding the modification and completion of specific normative acts as well as for the approval of fiscal-budgetary measures, as published in Official Gazette no. 44 of 17 January 2019. One possible solution would be the source taxation of firms through which they are traded.

In this case, we cannot accurately determine how many Romanians have invested or invest in virtual currencies and in what amount. Referring to the approximate volume over the last six months of the RON transactions to the total volume of transactions in all other currencies over the past six months, we can see that 845.5 Bitcoins were purchased with RON on the LocalBitcoins market, with a daily average of 32.5 Bitcoins, out of a total of 18,070,900 Bitcoins traded, with a daily average of 72,280 Bitcoins recorded by platforms like Bitfinex, Coinbase, Kraken and so on. It follows that a percentage $\alpha = 0.000468$ of the total volume of cryptocurrencies transactions is linked to the national currency. Of course, these estimates do not include the operations of the Romanians who chose to use euros, dollars, or other international exchange currencies, that is, the number of people who traded virtual currencies after calling for the exchange in another accepted currency as the reference currency and the double conversion rate applied to currency conversions. Figure 6 captures the interest in Bitcoin in Romania from the beginning of 2014 to the end of 2020. It can be noted that the evolution was similar to the worldwide one, the turning point of the Great Crash Crypto being felt at the same impact for Romania.

Figure 6. The evolution of Bitcoin in Romania, 2014–2020. Source: bitcoinromania.ro.

Metcalfe's law says that the value of a network is proportional to the square of the number of users connected to the system. Cryptocurrency networks can be compared to social networks, which means that the evolution value is directly proportional to engagement. More than 90% of Bitcoin movements can be explained by this law, using the square of the number of users and the average of transaction values performed. In the long run, this model may not be stable, since the number of users may vary considerably and the estimate for a large interval may not be in line with reality.

On the Coin Dance platform it is estimated that over 90% of the users are male, almost 50% aged between 25–34 years, confirming the wariness of older people against risk or innovation and the rapid assimilation of modern technologies by those younger, the phenomenon being considered an innovation trend of the Millennial generation, also known as Generation Y, which includes people born after 1980.

Positions regarding cryptocurrencies are different. Sweden and Denmark see a solution for storing values in the context of eliminating the physical currency. According to an article written in The Fintech Times (2018), Finland classified Bitcoin as a financial service and as a property in Australia.

A virtual currency regulated by a central bank is assumed to operate on the same principle as Bitcoin, with individuals or companies having a unique address for identification that is needed for transactions. The significant difference comes from banks and the other financial institutions agreeing that a central bank will hold the system (or the ledger), with the location where the transactions and the accounts are recorded. The currency distributed in this system may correspond to a traditional national currency (e.g., leu, euro, dollar) with the same status to maintain its value. Financial institutions would maintain their role in the economic system, through this method by replacing miners, known as people who keep the blockchain system up-to-date and investing computing power to solve cryptographic problems in exchange for new virtual currencies. Once transactions are confirmed, they become public, transparent, irreversible, and subject to audit.

The evolution of cryptocurrencies is generally dictated by quotes that reflect demand and offer for predefined periods. Of the more than 1000 virtual currencies that continually dispute their market shares, many disappear after launch. Others are supported by government bodies and are used declaratively as tools to regulate economic imbalances. Introducing and running them in financial circuits, like any other, facilitates routing to areas that are assimilated with cybercrime, money laundering, and financing terrorism, or to areas that make it possible to obtain undue profits. The connection between cryptocurrencies and ransom requests as a result of the ransomware attacks is no longer something unknown: only the methods change, but the goal remains the same.

This aspect is also highlighted by recent attack techniques, which consist of taking control by diverting or hijacking the mobile phone service and data transfer of one or more victims to devices managed by criminals without the knowledge or authorization of the account holder. Account synchronization gives almost total access to the fraudulent person to both mail, financial applications, and sensitive information that may affect privacy. Unique codes sent through SMS or delivered using

automatic calls including authentication are available to persons other than those to whom they were legally intended. The monetization of information is generally subordinated to the anonymization principle and thus we cross into the cryptocurrencies assimilated as target elements or components of an exchange gear. On one of the online stores, several applications for cryptocurrency fake wallets, which mimic the original services pages, were loaded. Immediate removal measures were taken after referral, but the reasonably high availability of nearly twelve months facilitated more than five thousand installations.

This subject is approached from several perspectives, and manufacturers exploit its controversial side, software facilities, and filters made available by the latest devices covering a wide range of customer requests. The need for security is on the second level at the base of Maslow's pyramid and is strong at the time of an election. The security of the digital wallet or the desire not to be in any way involved in adjacent activities has made the segregation very clear, and the percentages appear in the marketing plans. With a smartphone, you can communicate, download apps, connect to various servers, and you can, of course, manage your "financial" resources. According to a study made by Gian Volpicelli for WIRED, a technology magazine from UK, in (Volpicelli 2018), the trend is toward a blockchain smartphone, but there are situations where the theft or destruction of the phone is equivalent to the loss of credentials and automatic loss of access to the virtual deposit. Rescue distributed on different physical or cloud compartments of different parts of encryption keys has become an alternative to maintaining on a chip in quarantine and promises to rebuild these in the event of an accident. The settings allow you to activate or block all of the operating functions.

Evolving to meet societal needs, money is associated with value. Otherwise, it would have just become a symbol represented by a piece of printed paper or a digital token. Economists identify money with a verifiable asset, one of the attributes being to act as an accounting unit without which buyers and sellers cannot measure the value of a good or service (Mersch 2018). Compared to the traditional system, cryptocurrencies have two significant limitations. One is the lack of scalability, and the other is the uncertainty about the end of the transaction, the fragmented or segmented nature of the markets introducing new complications. We face an apparent rigidity, a lack of flexibility of systems and of crypto-infrastructures as long as it is not guaranteed that payment is final and irrevocable. Officially, in the most permissive scenario, cryptocurrencies are perceived as transferable assets (Shin 2018), decentralized technology being a poor financial substitute, regarded indulgently as the golden nuggets obtained with much effort and very good luck in the middle of the nineteenth century and, in the case of more demanding approaches, they are categorized as a combination of a soap bubble, a Ponzi scheme, and an ecological disaster. A (speculative) bubble is interpreted as a deviation of the price of an asset from its fundamental value. The irrational investment snowball rolls at a rate high enough to send an alarm signal to intelligent investors and it can be said that addressing a regulation is "asymmetric paternalistic if it creates advantages for those committing errors, not imposing constraints on those who are fully rational" (Juurikkala 2012; Sherman 2018).

The Venn diagram (Bech and Garratt 2017) illustrates the four key-properties of money: the issuer (e.g., the central bank); the form (e.g., digital or physical); accessibility (e.g., broad or restricted); and technology (e.g., based on accounts or token).

To fulfill the mandate, which implies, among other things, the maintenance of financial stability, central banks have an active role in supervision and, in some cases, in the provision of the payment system infrastructure. Even though the "mass" of cryptocurrencies is rather low in weight and too small to be considered systemic, this can change, and public authorities are aware of the potential risks induced and the effect on resilience. The risk of manipulating and changing levels is quite high given that the presumed proportion of holdings is inversely proportional to the owners. The emergence of crypto-assets requires, among other things, political decisions. There are sensitive issues regarding the possible issuance of cryptocurrencies other than conventional digital currencies by central banks. It is implicitly necessary for a coordinated approach at the global level to prevent abuses and to limit interconnections with regulated financial institutions and the risk of contamination (e.g., immature

technologies or superficial business models that can cause chain reactions) cannot be ignored. One of the members of the Executive Board of the European Central Bank noted the abundance of problems, and, in that context, it was pointed out that it is inappropriate to ignore the apparent coincidence of Bitcoin's launch period, a few months after the Lehman Brothers collapse in 2008.

Moreover, a particularly interesting study, already cited in the literature review (Corbet et al. 2019), draws attention to the increasing volatility of cryptocurrencies during periods of stress to the detriment of yield stability. The authors tried to highlight the destabilizing effects of cybercrime, the different ways in which quotations are affected, and the impact felt on prices. Some of the factors that influence the evolution of the market and the changes in the correlation between cryptocurrencies are dependent on informatic events (e.g., wallet hacking, computer frauds, etc.) and serious negative reputational events, which lead, among others, to a decrease in the level of investor confidence.

Views related to the term "money" may change, but we believe that one of the challenges will be in close connection to lending or guaranteeing, interest, and taxation services. In this research, Bascand presents his views related to this subject (Bascand 2018). Even though cash still occupies an essential share in the preference of the population and has proven its usefulness over several thousand years, it is not excluded to witness its reinvention in a digital form, but to impose itself, the functions fulfilled must bend over social constructions that call for the modification of technological frontiers. The time horizon is difficult to estimate. The form in which they will be incorporated into the banking system, if they are incorporated, will depend on the transformations dictated by the repositioning of financial bodies and the ability to synchronize. The dilemma is also strategic. There are few ways to recover your investment in the case of loss or destruction of credentials. Many packages remain locked and cannot be reintroduced into the circuit. They appear to be valid, but can no longer be traded, an inert mass whose percentage changes the indicators and graphs. The unstable degree of volatility over a day, and even more so for a longer period as well as a lack of correlation with the volume of officially unregistered holdings, influences any attempt of mathematical analysis. We believe that only one based on probability theory may approach the truth. However, one bold author has tried to formulate a fascinating model, but was limited by the terms taken into account and by the sources accessed (Kakushadze 2018). This is why we do not make any predictions in this study. However, we try to capture some essential arguments in motivating the steps meant to have the finality of transposing the proposals into standards and regulations.

6. Conclusions

To conclude our study, we highlight that the storage and processing of information spaces are at the forefront of the attackers' preferences, and there are gaps in regulations, similar to those in the cryptostream area. There are very few companies covering the risk of data corruption or compromising privacy, just as there are very few companies that provide the risk of volatility of cryptocurrencies. The fraudulent outflow of information packs, coupled with concerted intervention on quotations and counterfeiting of indicators, are possible attributes of manipulating a financial market. The term "financial market" may have different connotations, its influence being likely to manifest itself on one or more components of the set of values. Primary ingredients are to be dissolved to combat the complex, concentrated, or distributed effect. Therefore all evaluation steps should include an audit chapter, but it is impossible to foresee in the absence of precise, classifiable, input and output data.

Jurisdictional competencies or, more precisely, undefining them clearly, also induce constraints that should be eliminated. The link between cybercrime and cryptocurrencies is biunivocal, and therefore, the regulations in the field of cryptocurrencies must be harmonized with those in the field of cybercrime. The rights and responsibilities of international bodies need to be reviewed in the sense that they have the legal framework and the tools to allow them to intervene promptly to prevent, avoid, or counteract criminal slippage.

Distributed Ledger Technology has great potential to revolutionize the way activities can be coordinated and offers many benefits. However, the step from exploration to implementation must

first be tested on the test environment and on models that allow for real-life simulation. All public or private entities should be interested in identifying the best forms of collaboration to ensure security and stability. The role of central banks in this context is decisive while encouraging competition and cooperation.

The contribution that we consider to bring to the literature of the studied field is the summary of what has been studied and a great opening of a new path to empirical studies related to the interferences between cryptocurrency and cybercrime. The approached topic lends itself to more detailed development, which is why it remains a topic of future research. Our study is limited by the lack of consolidated and verifiable data in the field of cryptocurrencies and especially in terms of the influence of cryptocurrencies in cybercrime. We intend to identify suitable methods in the future to substantiate our finding both in the study of the impact of cybercrime in the evolution of cryptocurrencies, and of the influence of cryptocurrencies in cybercrime.

Author Contributions: Conceptualization, M.C.Ș. and S.L.C.; Methodology, M.C.S. and S.L.C.; Formal analysis, I.B.; Investigation, M.C.Ș., I.B., and M.V.A.; Resources, I.B.; Data curation, M.C.Ș. and S.L.C. Writing—original draft preparation, M.C.Ș.; Writing—review and editing, M.C.Ș., I.B., and M.V.A.; Visualization, M.V.A.; Supervision, M.V.A.; Project administration, M.V.A.; Funding acquisition, M.C.Ș. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the grant POCU 380/6/13/123990, co-financed by the European Social Fund within the Sectorial Operational Program Human Capital 2014–2020.

Conflicts of Interest: The authors declare no conflict of interest.

References

AARP. 2020. Cryptocurrency Fraud. Available online: https://www.aarp.org/money/scams-fraud/info-2019/cryptocurrency.html (accessed on 9 August 2020).

Auer, Raphael, and Stijn Claessens. 2018. *Regulating Cryptocurrencies: Assessing Market Reactions*. Basel: Bank for International Settlements Quarterly Review, September.

Bank for International Settlements. 2018. *Promoting Global Monetary and Financial Stability*. Annual Economic Report. Basel: Bank for International Settlements, June.

Bascand, Geoff. 2018. In Search of Gold: Exploring Central Bank Issued Digital Currency. Paper presented at The Point Conference, Auckland, New Zealand, June 26.

Bech, Morten, and Rodney Garratt. 2017. *Central Bank Cryptocurrencies*. Basel: Bank for International Settlements Quarterly Review, September, pp. 55–70.

BitScreener. 2018. Aurus.io, the Groundbreaking Startup Uses Blockchain to Create A Decentralized Global Standard Gold Currency. Press Release. February 15. Available online: https://bitscreener.com/news/aurus-io-the-groundbreaking-startup-uses-blockchain-to-create-a-decentralized-global-standard-gold-currency (accessed on 17 June 2020).

Bouri, Elie, Roubaud David, and Shahzad Syed Jawad Hussain. 2019. Do Bitcoin and Other Cryptocurrencies Jump Together? *The Quarterly Review of Economics and Finance*. [CrossRef]

Business Insider. 2019. Top Cryptocurrency Scams of 2019—And How Most Hackers Got Away with It. Available online: https://www.businessinsider.com/the-biggest-cryptocurrency-scams-and-arrests-of-2019-so-far-2019-8 (accessed on 9 August 2020).

Caporale, Guglielmo Maria, Woo-young Kang, Spagnolo Fabio, and Spagnolo Nicola. 2019. Non-Linearities, Cyber Attacks and Cryptocurrencies. *Finance Research Letters* 32: 101297. [CrossRef]

Chu, Jeffrey, Yuanyuan Zhang, and Stephen Chan. 2019. The Adaptive Market Hypothesis in the High Frequency Cryptocurrency Market. *International Review of Financial Analysis* 64: 221–31. [CrossRef]

CoinDesk. 2020. How to Spot a Crypto Scam. Available online: https://www.coindesk.com/how-to-spot-a-crypto-scam (accessed on 9 August 2020).

Corbet, Shaen, Douglas J. Cumming, Brian M. Lucey, and Peat Maurice. 2019. The Destablishing Effects of Cryptocurrency Cybercriminality. *Economics Letters* 191: 108741. [CrossRef]

Corbet, Shaen, Larkin Charles, and Lucey Brian. 2020. The Contagion Effects of the COVID-19 Pandemic: Evidence from Gold and Cryptocurrencies. *Finance Research Letters* 35: 101554. [CrossRef]

Desjardins, Jeff. 2017. All of the World's Money and Markets in One Visualization. *The Money Project*. October 26. Available online: http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/ (accessed on 25 March 2020).

Erste Group. 2018. Erste Group and ASFINAG Successfully Launch Europe's First Entirely Blockchain-Based Capital Markets Issuance. Available online: https://www.erstegroup.com/en/news-media/press-releases/2018/10/23/paperless-ssd-blockchain-alias (accessed on 23 October 2018).

Gandal, Neil, James Hamrick, Moore Tyler, and Oberman Tali. 2018. Price Manipulation in the Bitcoin Ecosystem. *Journal of Monetary Economics* 95: 86–96, Online Supplementary Material 20 December. Available online: https://ars.els-cdn.com/content/image/1-s2.0-S0304393217301666-mmc1.pdf (accessed on 25 March 2020).

Griffin, John M., and Amin Shams. 2018. Is Bitcoin Really Un-Tethered? *The Journal of Finance* 75: 1913–64. [CrossRef]

Grobys, Klaus, Ahmed Shaker, and Sapkota Niranjan. 2019. Technical Trading Rules in the Cryptocurrency Market. *Finance Research Letters* 32: 101396. [CrossRef]

Juurikkala, Oskari. 2012. The Behavioral Paradox: Why Investor Irrationality Calls for Lighter and Simpler Financial Regulation. *Fordham Journal of Corporate & Financial Law* 33: 40–42.

Kakushadze, Zura. 2018. Cryptoasset Factor Models. *Algorithmic Finance* 7: 87–104. [CrossRef]

Kaspersky. 2020. 4 Common Cryptocurrency Scams and How to Avoid Them. Available online: https://www.kaspersky.com/resource-center/definitions/cryptocurrency-scams (accessed on 9 August 2020).

Khatwani, Sudhir. 2018. 7 Most Common Types Of Cryptocurrency Scams & Tips to Avoid Them. *Consutra*. October 15. Available online: https://coinsutra.com/cryptocurrency-scams/ (accessed on 9 August 2020).

Koerhuis, Wiebe, Kechadi Tahar, and Le-Khac Nhien-An. 2019. Forensic Analysis of Privacy-Oriented Cryptocurrencies. *Forensic Science International: Digital Investigation* 33: 200891. [CrossRef]

Mersch, Yves. 2018. Virtual Currencies Ante Portas. Paper presented at 39th Meeting of the Governor's Club of The Central Asia, Black Sea Region and Balkan Countries, Bodrum, Turkey, May 14.

PYMNTS. 2018. ICO Investors Fall For Exit Scams, Phishing. *Cryptocurrency*. August 15. Available online: https://www.pymnts.com/cryptocurrency/2018/ico-investors-exit-scams-phishing-attempts-bitcoin-ethereum/ (accessed on 17 June 2020).

Robby, Houben, and Alexander Snyers. 2018. *Cryptocurrencies and Blockchain, Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*. PE 619.024. Brussels: European Parlament, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, July.

Sherman, Nathan J. 2018. *A Behavioral Economics Approach to Regulating Initial Coin Offerings*. Georgetown University Law Center, J.D. expected May 2019; University of Richmond, B.S.B.A 2016. Available online: https://georgetownlawjournal.org/articles/280/behavioral-economics-approach-to/pdf (accessed on 20 June 2020).

Shin, Hyun Song. 2018. *Cryptocurrencies and the Economics of Money*. Bank for International Settlements lecture on the occasion of the Bank's Annual General Meeting in Basel. Basel: Bank for International Settlements, June 24.

Staff of Global Legal Research Directorate. 2018. *Regulation of Cryptocurrency Around the World*; Washington, DC: The Law Library of Congress, Global Legal Research Center, United States.

The Fintech Times. 2018. 7 Bitcoin-Friendly Countries That Welcome Cryptocurrency Investments. *Newsletter*. July 4. Available online: https://thefintechtimes.com/7-bitcoin-friendly-countries-that-welcome-cryptocurrency-investments/ (accessed on 25 March 2020).

Volpicelli, Gian. 2018. HTC Has Made a Blockchain Phone that Cryptocurrency Fans Will Hate. *WIRED*. November 2. Available online: https://www.wired.co.uk/article/htc-exodus-crypto-phone (accessed on 25 March 2020).

Xu, Qiuhua, Yixuan Zhang, and Ziyang Zhang. 2019. Tail-Risk Spillovers in Cryptocurrency Markets. *Finance Research Letters*. in press. [CrossRef]

ZD Net. n.d. China Arrests over 100 People Suspected of Involvement in PlusToken Cryptocurrency Scam. Available online: https://www.zdnet.com/article/china-arrests-over-100-people-suspected-of-involvement-in-plustoken-cryptocurrency-scam/ (accessed on 9 August 2020).

Zellweger-Gutknecht, Corinne. 2018. Developing the Right Regulatory Regime for Cryptocurrencies and Other Value Data. In *Private and Public Law Implications of Cryptocurrencies*. Edited by David Fox and Sarah Green. Oxford: Oxford University Press, August.

Zhang, Yuanyuan, Stephen Chan, and Jeffrey Chu. 2018. Nadarajah Saralees. Stylised Facts for High Frequency Cryptocurrency Data. *Physica A* 513: 598–612. [CrossRef]