Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments

Article *in* Sensors · March 2023

DOI: 10.3390/s23063155

4 authors:

Paweł Weichbroth
Gdansk University of Technology
110 PUBLICATIONS **952** CITATIONS
SEE PROFILE

Kacper Wereszko
Gdansk University of Technology
14 PUBLICATIONS **45** CITATIONS
SEE PROFILE

Helena Anacka
Gdansk University of Technology
16 PUBLICATIONS **74** CITATIONS
SEE PROFILE

Jolanta Kowal
University of Wrocław
126 PUBLICATIONS **577** CITATIONS
SEE PROFILE

sensors

MDPI

Review

Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments

Paweł Weichbroth [1,*], Kacper Wereszko [2], Helena Anacka [3] and Jolanta Kowal [4]

[1] Department of Software Engineering, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland
[2] Department of Algorithms and System Modeling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland
[3] Faculty of Management and Economics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland
[4] Institute of Psychology, University of Wrocław, Dawida 1, 50-529 Wrocław, Poland
* Correspondence: pawel.weichbroth@pg.edu.pl; Tel.: +48-58-347-29-89

Abstract: [Context] The goal of security is to protect digital assets, devices, and services from being disrupted, exploited or stolen by unauthorized users. It is also about having reliable information available at the right time. [Motivation] Since the inception in 2009 of the first cryptocurrency, few studies have been undertaken to analyze and review the state-of-the-art research and current developments with respect to the security of cryptocurrencies. [Purpose] We aim to provide both theoretical and empirical insights into the security landscape, in particular focusing on both technical solutions and human-related facets. [Methodology] We used an integrative review which could help in building science and scholarly research, the basis for conceptual and empirical models. [Results] Successful defense against cyberattacks depends on technical measures on the one hand, as well as on self-education and training with the aim to develop competence, knowledge, skills and social abilities, on the other. [Contribution] Our findings provide a comprehensive review for the major achievements and developments of the recent progress on the security of cryptocurrencies. [Future research] Since there is increasing interest in adoption of the current solutions within the central bank digital currencies, the future research should explore the development and inception of effective measures against social engineering attacks, which still remain the main concern.

Keywords: security; digital currency; cryptocurrency; wallet; architecture; data transmission method; social engineering attack; countermeasures

Citation: Weichbroth, P.; Wereszko, K.; Anacka, H.; Kowal, J. Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments. *Sensors* **2023**, *23*, 3155. https://doi.org/10.3390/s23063155

Academic Editors: Zeinab Shahbazi and Faisal Jamil

Received: 28 January 2023
Revised: 10 March 2023
Accepted: 13 March 2023
Published: 15 March 2023

1. Introduction

The Digital Revolution, also known as the Third Industrial Revolution [1], undoubtedly marks the beginning of the Information Era. The advancement of technology from analog electronic and mechanical devices to digital technology has been remaking the world [2]. This digital revolution has proceeded at breakneck speed since no other human invention has reached more people in as short a space of time as the Internet [3].

The rise of the Internet has changed the way people exchange not only information [4] but also other goods [5], including money. Due to the limitations of local currencies, concerning limited liquidity, proxy transaction costs for foreign payments, and emerging economies' trust deficit, to name a few, the first cryptocurrency emerged just over a decade ago to overcome these obstacles.

By design, cryptocurrencies (or simply crypto) facilitate peer-to-peer payments without the oversight of an intermediary (such as a bank or any governmental body) [6], and eliminate the need for identification information for both parties [7]. In general, cryptocurrencies and their underlying technology (blockchain) are seen as a source of a radical shift to the "Internet of Value", which can disrupt the traditional financial world [8]. Despite

surging in popularity and being recognized as the most trusted financial instrument by many investors [9], whether crypto will ever go mainstream depends on factors such as price stability, ease of use and security [10].

Indeed, the issue of cybersecurity always brings considerable attention when using cryptocurrencies. According to the Federal Trade Commission, the number of cryptocurrency scams has increased sharply from October 2020 through March 2021, with nearly 7000 people reporting losses totaling more than $80 million. To be clear, the top scams, considering their value and impact, hit business organizations and government bodies. For instance, in February 2014, hackers stole about $460 million in bitcoins from Mt. Gox exchange [11], the world's largest bitcoin trading exchange with its headquarters in Tokyo. After admitting the 850,000 Bitcoin loss, the exchange was shut down just weeks later, causing the first Bitcoin market crash, as its price slid from $800 to $400 [12]. As we know now, it was not the first organization to suffer a massive theft, and will definitely not be the last.

The ISO/IEC 27032 standard defines cybersecurity as "preservation of confidentiality, integrity and availability of information in the Cyberspace" [13]. In turn, Cyberspace is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form". Inarguably, with the introduction of cryptocurrencies, new cybersecurity issues have emerged [14–16], reshaping and redefining its landscape. Since understanding cybersecurity is no longer optional for businesses and individuals, this study delves into this topic by reviewing and analyzing the state-of-the-art research and current developments.

To the best of our knowledge, few attempts (if any) have been made so far to undertake a similar study. In particular, our study tackles the ongoing discussion on crypto cybersecurity (or simply security) by adopting the grounded theory approach developed by Glaser and Strauss [17], in particular by adapting analytical thinking [18] and sampling strategies [19]. Taking into account the general notion of cybersecurity, in our view, its multidimensional nature considered in the context of cryptocurrencies can be further conceptualized within two mainstream areas, namely: technological and human. In particular, the former concerns four interconnected hardware and software domains, spanning from cryptocurrency wallets to security architectures, models, and data transmission methods. In contrast, the latter considers humans (users) as the last link of the security chain. It should be noted here that the notion of a user is a theoretical lens to consider cybersecurity in terms of social engineering attacks and corresponding countermeasures [20], hence these are also investigated in our study.

While the grounded theory suggests a contextualized understanding of the phenomena [21], we collected, coded and analyzed the data based on an extracted set of keywords (marked in italics). To explore these five topics, we selected and applied guidelines elaborated by Kitchenham and Charters [22]. This methodology, along with its associated principles, has been well received by researchers worldwide, and nowadays is widely adopted not only in the computer science domain. A systematic search was performed on Scopus and Google Scholar using their available online search engines. We also used Google Search to acquire recent market and statistical data. In formulating search queries, we used combinations of the keywords, indicating the relationships between them by specifying explicit logical operators such as AND, OR and NOT [23]. Initially, from the list of the search results, potentially relevant papers were selected, based on an individual evaluation of both the title and abstract. The criteria followed in assessing the quality of a paper were the relevance of its topic, objective and outcome. To ensure that findings were properly classified and synthesized, at least two other authors checked and confirmed their validity.

The rest of the paper is organized as follows. In Section 2, we discuss the background of the development of cryptocurrencies. In Section 3, we define and classify crypto wallets. In Section 4, we review and analyze security architectures, followed by a description and

exemplification of the related models given in Section 5. Afterwards, in Section 6, we recognize and localize the data transmission methods developed for blockchain-based solutions. Next, in Section 7, we elaborate on the adopted social engineering attacks and adapted countermeasures for the cryptocurrencies settings. In Section 8, we discuss the findings, including the implications for theory and practice. Eventually, in Section 9, we conclude the paper with a summary of the performed study.

2. Background

The Merriam-Webster dictionary defines a cryptocurrency as "any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions" [24]. In other words, cryptocurrency is "a digital currency produced by a public network, rather than any government, that uses cryptography to make sure payments are sent and received safely" [25].

There are various ways to mine cryptocurrency:

- Application-Specific Integrated Circuits (ASIC) are a special type of microchip designed to perform a repeated function that hashes blocks in order to find a valid Proof-of-Work [26].
- Central Processing Unit (CPU) utilizes one or more processors and thus is poorly profitable for its users [27].
- A Graphics Processing Unit (GPU) utilizes one or more graphics cards [28] and is currently claimed to be the most popular and well-known method of cryptocurrency mining [29].
- Field-Programmable Gate Array (FPGA) is an electronic circuit that one can program to execute certain logical operations with a programming language such as Verilog or VHDL. FPGAs are more adaptable than ASICs, and faster and more efficient than GPUs [30].

Considering the number of the number of mining participants, the mining process can be performed in two scenarios: individually (solo mining), or in a group (mining pools). Another approach is cloud mining in which computational work from a cloud-computing farm is outsourced. Here, the mining process is easier to implement since it does not require specialized hardware deployed. Nevertheless, cloud computing imposes a number of security issues, including access control, authentication and identification, availability, policy integration, and audit strategies, as well privacy concerns such as unauthorized secondary usage, lack of user control, and unclear responsibility, just to name a few [31].

Although Bitcoin is claimed to be the first established cryptocurrency, there had been preceding attempts at developing digital currencies with ledgers secured by reliable encryption methods. Two examples of these are Bit Gold, invented by Nick Szabo in 1998, and B-Money, introduced by Wei Dai in the same year. However, they were never fully developed and put on the marketplace [32]. Ten years later, on 31 October 2008, the nom de plume Satoshi Nakamoto posted a paper to a cryptography mailing list, entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" [33]. Afterwards, on 11th January 2009, the first bitcoin transaction occurred when Nakamoto sent 10 bitcoins (BTC) to a computer programmer, Hal Finney [34].

On 15 August 2010, one of the most striking security issues in the blockchain network appeared, involving a transaction of 184 billion BTC, well beyond the 21 million supply cap, and 8784 times more than should ever exist [35]. Within five hours of the discovery, Nakamoto released a new version (0.3.1) of the Bitcoin client, with a fix containing a soft fork. As a consequence, two different versions of Bitcoin existed in the immediate hours after version 0.3.1 was published. Eventually, the network made the previously valid blocks that included the exploited transactions invalid. Nineteen hours after the disclosure of the incident, the "good" chain became the dominant one, however the "bad" chain still existed

and disrupted some users for at least the next day [36]. Ultimately, the chain introduced in this fixed version became the Bitcoin blockchain that exists today.

Later that year, a programmer named Laszlo Hanyecz bought two pizzas for 10,000 bitcoin at Papa John's pizza [37], enabling a monetary value to be attached to BTC for the first time. Back then, Bitcoin's price stood at less than a penny, while at today's prices, they would be worth more than 430 million USD. In November 2020, Bitcoin processed around 293,000 daily transactions. By August 2021, 18.7 million bitcoins were still available, which leaves roughly 2.3 million yet to be introduced into circulation, while that last bitcoin will be delivered somewhere in February 2140 [38]. In November 2021, the Bitcoin market capitalization reached over 1148 billion U.S. dollars.

Obviously, there are other cryptocurrencies available on the market, and among the first to emerge were Namecoin (NMC) and Litecoin (LTC). The former is the first cryptocurrency that acts as a decentralized domain name system [39], while the latter is considered as the "silver standard", becoming the second most accepted crypto by both exchanges and miners [40]. In 2021, it is estimated that there were over 6000 cryptocurrencies [41], with a total capitalization of 1538 billion U.S. dollars (excluding BTC) as of November 2021 [42]. By the end of February 2023, there are over 22 k cryptocurrency projects, with the total value of 1 trillion U.S. dollars, where ten largest cryptocurrencies by market capitalization are: Bitcoin ($452.1 billion), Ethereum ($200.0 billion), Tether ($70.9 billion), Binance Coin ($47.9 billion), U.S. Dollar Coin ($42.4 billion), XRP ($19.3 billion), Cardano ($12.6 billion), Dogecoin ($10.8 billion), Polygon ($10.7 billion), and Binance USD ($10.6 billion) [43].

The skyrocketing growth of the global crypto market value has attracted not only honest investors but also scammers. Generally speaking, cryptocurrency scams fall into two different categories, namely: data breach, and disinformation [42]. By definition, a data breach is a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed" [44]. It should be noted here that we will use a more general term later on, namely a security breach, since this naming covers a wider spectrum of objects, including applications, services, networks and hardware devices [45]. The second category of scams concerns disinformation, that is, false or inaccurate information, deliberately spread to deceive or mislead [46]. By nature, intentionally, maliciously deceptive information is created and spread with the aim of tricking cryptocurrency investors, intended to result in financial or personal gain, hereafter termed fraud [47].

With waning trust in local currencies, facilitated by the proliferation of social media, the estimated number of global crypto users passed 106 million in February 2021 [48], which means a rise by more than 881% compared to the past year. The top three reasons are that it is easy to make trades, it is exciting to invest in, and there is potential for high growth in a short period of time [49]. However, these premises have brought about new threats, imposing a significant impact on financial stability for not only the individuals but also for the global economy as well. As security breaches and fraud schemes have become increasingly sophisticated, modern security measures have become less and less efficient, lacking the ability to provide an adequate level of protection.

3. Cryptocurrency Wallets

A cryptocurrency (or digital currency) wallet (CW) is an application that generates and stores a pair of cryptocurrency private and public keys [50], facilitating the transfer of funds between individuals [51]. In particular, CWs are used to manage the user's digital assets, including creating an account address, managing cryptocurrency transactions, supporting queries of transaction records, as well as other basic financial services [52]. Interestingly, digital currency wallets, as may be suggested by the name, do not store digital currencies [53].

The most general classification distinguishes two types of cryptocurrency wallets:

- Custodial wallet in which the private keys are held by a third party organization,

- Non-custodial wallet in which all the blockchain custodian services resides with its user.

Some authors point out that the former may be considered less secure than the latter [54]. Nevertheless, custodian wallets are claimed to be the best entry point for users who lack a technical understanding of blockchain technology, impose less responsibility and are usually more convenient to use [55]. On the other hand, a non-custodial wallet delivers a spectrum of security-based benefits, enabling the user to solely possess the private key with its associated public address. Typically, this takes the form of either a file or "mnemonic phrase" of between 12 and 24 randomly generated words. This feature enables the user to conduct private P2P crypto trades, in particular trades on assets that are not listed on custodial crypto exchanges [56]. Both custodial and non-custodial wallets are available in three different settings: hot, cold, and hybrids (of the two above).

A hot wallet (HW) is always connected to the Internet 100% of the time, allowing a user to send and receive digital assets on demand. However, due to the instant connection, a hot wallet is vulnerable to attack by malware or hacker. Thus, holding a large amount of digital assets in a hot wallet seems to be a poor security practice. Based on the technology used, three different types of HWs are distinguished [57]:

- Desktop wallet (e.g., Atomic Wallet, Eidoo, Exodus) is a piece of software that can be downloaded and installed on a personal computer (desktop, laptop); it is claimed that this scenario offers one of the maximum tiers of security.
- Online wallet (e.g., Coinbase, GateHub, Guarda) is a web-based software application [58], located and executed remotely in a service provider's cloud environment.
- Mobile wallet (e.g., Edge, Coinomi, Enjin) is a stand-alone application devoted to mobile devices (e.g., smartphones, tablets) [59].

In contrast, a cold (or hardware) wallet (CW) (e.g., Corazon, Keepkey, Sugi) is designed to generate and store a user's private keys in an offline environment, known as cold storage. They are usually implemented as USB-based plugin devices, which appear to their user as similar to USB drives. A cold wallet, based on an off-line hardware solution secured by a passcode or any other additional authentication means, is claimed to be significantly safer than software-only equivalents [60,61]. A rule of thumb is to use a CW to store a relatively large amount of digital assets, or to make regular savings into crypto as part of an investment portfolio.

Hybrid (Hot-Cold Hybrid, HCH) wallets (e.g., Exodus, Trezor) have emerged as trade-offs, seeking to find a balance between hot and cold wallets, by taking advantage of dual online and offline technologies [62]. In practice, HCHs enable the users to safely store a set amount of assets offline in cold storage, meanwhile also sharing an amount of crypto online for instant trading.

It should also be noted that, despite the digital nature of cryptocurrencies, one can also use paper wallets. Difficult to access and completely off-line, they take the form of printed sheets of paper with public keys and private keys printed out [60], mostly in QR Codes that need to be scanned to be used. In addition to the risk of fire, theft, loss, or water damage, there are other reasons paper wallets have become obsolete. A user must use a trusted wallet generator, but since numerous are open-source software, malicious hackers have developed modified versions available online that can steal the user's keys [63]. However, paper wallets are considered one of the most hack-proof wallets of all.

To sum up, the security level of the cryptocurrency wallet depends on its type, taking into account the key management schema. It seems rational to use cold wallets since their off-line design effectively protects the stored assets from being stolen [64]. On the other hand, since there is no limit to the number of wallets, one can split their assets across multiple wallets, diversifying them not only by the amount but on the type as well. Furthermore, a user's password policy should follow best practices, such as minimum password length, complexity and history enforcement, minimum and maximum password age [65]. Another primary concern is the design and scheduling of backup and recovery maintenance plans to respond effectively in the event of data loss [66]. From a user

perspective, it seems reasonable to recognize the impact of these issues on the security of cryptocurrency wallets.

4. Security Architectures

Security architectures could be defined as global systems essential to protect the IT infrastructures and technologies that are required to construct secure platforms [67]. According to Conrad et al. [68], security architecture is a complex concept that includes security components of software, hardware, and operating systems, as well as procedures that make it possible to build, adjust and evaluate those security components. Beyond this, further essential elements of security architecture include, inter alia, legal regulations, internal processes and procedures [69], integrated with other autonomous physical systems (e.g., fire protection, and anti-theft systems) [70].

When reviewing the existing architectures of digital currencies – the decentralized architecture of bitcoin is worth special attention [71]. A blockchain system and its child—a bitcoin cryptocurrency—are perceived as core digital architectural solutions. Bitcoin is currently the most popular cryptocurrency using blockchain; its architecture reduces the transaction and intermediary steps and costs by eliminating third parties, bank blocks, internal networks and transaction aggregators [33,72]. Based on blockchain, a traditional Bitcoin System of Systems (SoS) architecture is supported by the Bitcoin Network that consists of the Bitcoin Foundation, Bitcoin Payment Processors and e-stores using Systems Modelling Language, with an irreversible history of all Bitcoin transactions that is passed from the payer to the recipient, which makes it possible to verify the real owners of all Bitcoins [72].

Basically, blockchains are nothing more than databases, deployed and managed for the benefit of their owners [73]. In common sense, blockchain is the technology that underpins modern cryptocurrencies. More formally, according to IBM, blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network [74]. Transactions confirmed and validated through blockchain are immutable, while a transaction timestamp history is available for the wider blockchain user community, supporting the transparency, traceability and irreversibility of the blockchain technology [75]. The so-called "fingerprint attribute"—the uniqueness of each block in a chain—is fundamental to the blockchain architecture, while malicious attempts to swap blocks of data and modify their hashes would lead to the link breaking and the following blocks becoming invalid [76]. There are cryptocurrencies that are based on Blockchain 1.0 [77], e.g., Bitcoin, Dogecoin and Litecoin. Blockchain 2.0 is used on smart contracts and properties, while Blockchain 3.0 could have more general applications, from healthcare and educational institutions to scientific and governmental projects [78].

Blockchain is perceived as a safely encrypted ledger and a reliable system of cryptocurrency exchange [79,80]. The security of blockchain architecture is enhanced using a procedure called "proof of coinage" [81]. According to [79], in order to ensure cybersecurity and digital currency safety, blockchain technology should be further exploited. One of the possible solutions to preserve data safety and integrity is to utilize the metastable blockchain protocol that ensures greater security of blockchain platforms [82].

According to the World Bank, a distributed ledger refers to a novel and fast-evolving technology for recording and sharing data across multiple data stores, termed as ledgers, which are enablers for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants [83]. Distributed ledger technology (DLT) seems to be a promising approach, both addressing the limitations of the current digital identity methods [84] and applications deployment [85], at the same time being highly secure, transparent, and tamper-proof [86].

While there are a few high-tech solutions under DLT, such as hash-graph, holochain, tangle, side-chain and blockchain, which differ in terms of consensus algorithms and data storage methods, blockchain is the technology based on which cryptocurrencies arose [87]. In terms of an algorithm allowing a new block creation and mining within

blockchain, one can distinguish among: proof of stake (distinctive for EOS, Cardano (ADA) and Tron (TRX) [88]), proof-of-work (used in most popular cryptocurrencies, e.g., Bitcoin (BTC), Litecoin (LTC) and Ethereum (ETH) [89]) and proof-of-capacity mechanism (used in Ripple (XRP) and Signum (SIGNA) [90]). Additionally, proof-of-burn consensus algorithm allows the miners to "burn" coins without extensive energy consumption, thus preventing double-spending (e.g., Slimcoin [91]). All the mentioned algorithms aim at approving and validating transactions, thus ensuring the security and transparency of the respective blockchain [92].

DLT solves the problem of centralized supervision by peer-to-peer verification and multiple—instead of one—data storage locations [93]. Different blockchains can also differ in terms of permission strategies: those could be public, private, consortium, or hybrid ones [94]. Public blockchains are open to all, they are 'permissionless', with unlimited access to transactions history and mining, popular public cryptocurrencies examples of which are: Bitcoin, Litecoin, Ethereum, Dogecoin and Monero [95]. Private or 'permissioned' ones are restricted to a close smaller and controlled users' group with additional moderator's function (e.g., Enterprise, Hyperledger and Ripple) [96]. Finally, hybrid blockchains synthesize both private and public elements, with open history and smart contracts for verification; while consortium or 'federated' blockchains involve decentralized chain of users belonging to the organization and managed by pre-established nodes [97]. All those are examples of different blockchains that build up different mining, verification, storage and transactions solutions.

According to [79,81], blockchain technology is considered secure and stable, while its network architecture is changeable. For example, it is seen as a reliable response to the Internet of Things (IoT) security vulnerabilities (which could stem from application layer threats, network layer threats and physical layer threats [98]), through secure data sharing, secure authentication, access, and control of numerous IoT devices, as well as secure data storage [80]. The so-called consensus algorithm of blockchain is aimed at ensuring architecture safety [81]. A classical blockchain consensus protocol is intended to both eliminate possible faults and to guarantee the security of the blockchain [99].

Examples of blockchain security algorithms are corresponding consensus algorithms (e.g., proof-of-stake, delegated proof-of-stake, Raft, proof-of-work and practical Byzantine fault tolerance), which deal with potential distribution system problems (e.g., Byzantine Generals Problem) and are elaborated for different scenarios [81]. For instance, proof-of-work functionality is an algorithm to reach consensus in a network by using real processor cycles to create new blocks of blockchain, thereby verifying and protecting the blockchain history and preventing double-spending [72,100]. The Byzantine Generals Problem is applicable in case of the distributed systems compromise, and could be solved with the complex Paxos algorithm, or the simpler and more popular Raft algorithm [81]. On the other hand, to provide more secure identity management, one can also consider employing the most efficient encryption methods with the aim of optimizing user identity verification time [101].

Bitcoin is an electronic money system based on a reusable proof-of-work (PoW), which uses cryptographic controls with a scarce cryptocurrency supply and irreversible hard transactions performed with no centralized authentication, which provides user anonymity [72]. The traditional blockchain architecture consists of four layers: application layer, extension layer, network layer and data layer. However, the Bitcoin architecture cannot currently ensure perfect privacy protection at such high transaction rates [99]. For example, when the throughput is increased, the Bitcoin protocol is exposed to a double spend attack, as attackers could switch the chain and even replace it with one with a lower processing capacity [102]. Moreover, Bitcoin records do not ensure absolute transactional privacy, since there are methods to link the users' data (e.g., IP addresses) to their pseudonyms [103]. There are techniques to ensure better privacy of users' data, such as using a mixing service (e.g., Coinjoin [104]), unlinking transactions and their origins (e.g., Zerocoin [105]), and hiding the coins' values and amounts (e.g., Zerocash [103,106]).

To maintain the security architecture, three aspects need to be taken into consideration: data privacy and security, which is linked with social aspects; system security—related to technology and computing, as well as operating system security—aimed at counteracting digital fraud [69]. Essentially, the security of each of the systems' layers (infrastructure, network and application layers) needs to be guaranteed, while another important aspect is to ensure the availability, integrity and confidentiality of information and data [107]. The information security architecture is intended to ensure that the data are encrypted in a protected user device, the users are authenticated, the access is authorized appropriately, the logging is audited, and decryption and safe storage of data are ensured in a securely protected resource [108].

With the growing popularity of so-called Central Bank Digital Currencies, CBDC or digital money used for cross-banks settlements [109], there are endeavors to consider blockchain technology for CBDC purposes. While, according to Zhang and Huang [75], a permissioned blockchain, or a blockchain based on permissions is a better solution for Central Bank Digital Currencies, blockchain's limitations in terms of, e.g., scale, use scenarios, inter-operations and performance impose certain barriers on the use of the technology for CBDC [110]. Additionally, legal and procedural requirements, and the internal regulations of central banks, prevent the full-scale incorporation of decentralized technology based on anonymity, irreversibility and lack of compliance with external regulations [111].

Digital security is an integral part of the bigger digital infrastructure and network, therefore it should not be set up separately from the users, devices, the network and environment. Moreover, one security architecture cannot be a universal solution to different threat scenarios, which is why a so-called tier-based or reconfigurable security architecture that provides changeable security settings is preferable [112]. More specifically, the reconfiguration mechanism, which is a part of a security architecture, ensures monitoring of various characteristics to dynamically react and activate those security mechanisms that are more appropriate in a particular situation [113]. Additionally, a reconfigurable security architecture is a dynamic solution that is able to localize and detect cyberattacks, therefore ensuring the actual security warranty [114].

To sum up, the security architectures of digital currencies proposed by a wide range of research concentrate on blockchain technology, and especially on Bitcoin solutions, which are perceived as relatively secure, due to the reliable data access, storage, encryption and transfer arising from the blockchain architecture itself. However, security threats related to blockchain systems come from networks, software, and hardware fragility, as well as human factors. Potential solutions aimed at increasing blockchain security are the corresponding consensus algorithms, meta-stable blockchain protocol, external-internal security trade-off and more reliable network and software.

5. Security Models

In general, security models are used to define the notion of security embodied by a computer system [115]. McLean points out that security models have been applied to "describe any formal statement of a system's confidentiality, availability, or integrity requirements" [116]. In other words, three core ingredients, namely confidentiality, integrity, and availability, build up the CIA triad model [117], which is now widely recognized and typically adopted to address principal information security objectives [118].

The definition of confidentiality states that it is "the process of and obligation to keep a transaction, documents, etc., private and secret," or, in a more narrow sense, it is "the right to withhold information from others" [119]. In the context of cybersecurity, privacy means the freedom from damaging publicity, secret surveillance, public scrutiny, and any unauthorized disclosure of the user's personal data or information [120], while secrecy is the practice of maintaining privacy [121].

Thinking in the categories of a cryptocurrency system that requires the generation of cryptographic keys and seeds, a user needs to pay close attention to preserve their own privacy. On the other hand, having unguessable numbers obviously provides the first line

of defense against unauthorized access [122], but even more importantly, protects against unwanted actors impersonating the intended key (seed) holder [123]. Therefore, to mitigate risks concerning the unintentional disclosure of the wallet-holder's identity or stolen keys, one should follow best practices such as using keys (seeds) only in trusted environments and requesting a minimum of two signatures for performing transactions. It is worth noting here that the aforementioned fraudulent incident of Mt. Gox is believed to have occurred because the company involved did not use a multi-signature approach to store the private keys of the wallet-holders [124].

In the realm of security, integrity refers to the accuracy, consistency, and completeness of data [125]. Here, however, one question arises: what is the meaning of these three notions? First, accuracy is strictly related to the notion of the magnitude of an error [126]. Second, consistency is defined as the absence of any discrepancy between particular data values concerning the same object [127]; typically, data consistency is considered under three different dimensions [128]:

- Point-in-time consistency means that data is said to be point-in-time consistent if all related data is the same at any given instant in time.
- Transaction consistency means that the data must be in a consistent state before and after a single transaction is executed; if an error occurs, all submitted changes are rolled back and the data returns to the original state.
- Application consistency refers to the state in which all intra- and inter-related data are synchronized and represent the true status of applications.

For cybersecurity of cryptocurrencies, the blockchain is typically applied to systems that require both immutability and integrity checks [129]. By design, blockchain-based systems eliminate the requirement of a third-party trusted authority. Instead, to preserve the consistency and reliability of both the data stored and transactions performed, blockchain adopts a decentralized consensus mechanism and cryptographic security measures [130]. A consortium of multiple organizations can share the responsibilities of maintaining such a system [74].

However, a common misconception is that the use of a blockchain alone can ensure data integrity [131]. By defition, the data integrity involves preserving the accuracy, reliability and stability of data [132]. Even though blockchain has the capability of reliably preventing an undetected data modification once it has been confirmed on-chain, it will only enforce this mechanism on successfully-input data. In other words, if the data is not accurate at the time of input, then putting it on a blockchain does not benefit in any way, except in preserving its immutability. Unarguably, the old saying "garbage in, garbage out" is also valid here. Hence, defining and applying a data hygiene action plan is a critical precursor to any blockchain deployment, but this is still claimed by some to be hard to achieve in immutable settings [133].

From a user perspective, best practices regarding data integrity might concern the following precautions: (*i*) generating unique addresses for every transaction, (*ii*) checking identification, background of all key (seed) holders, and their references, (*iii*) storing keys which have signing authority in different locations. In fact, the blockchain inherently shifts all the integrity responsibility to the user since there are no internal auditing routines regarding data checks against errors, fraud, illegal acts or key losses. Regarding the last problem mentioned, if the cryptographic keys are compromised, the identity of the individual (or any other entity) is lost, and can be abused in many ways, potentially resulting in considerable damage [134].

Moreover, security policies such as a separation of duty (SoD) [135] and the principle of least privilege (PoLP) [136], as well as internal audits, and external audits [137] including also governmental bodies (e.g., Internal Revenue Service (IRS) [138]), offer assurances to the investors, shareholders and owners.

The last ingredient of the CIA model is availability. The general notion states that availability means the quality or state of being easy or possible to obtain, or being ready for use [139,140]. While the above definition seems not to be difficult or elusive to un-

derstand, its explication takes different forms in the computer science and other related disciplines [141]. Having said that, below, we provide only some of its definitions, but those that are widely recognized and referred by both theory and practice.

- In the context of the criteria for evaluating computer security provided in the Information Technology Security Evaluation Criteria (ITSEC), availability means prevention of the unauthorized withholding of information or resources [142].
- In the context of the fundamental objectives of information security defined in the Federal Information Security Management Act (FISMA) availability aims at ensuring the timely and reliable access to and use of information [143].
- Along with integrity and confidentiality as the basic security properties and the targets of security threats, availability is the ability of a system to ensure that an asset can be used by any authorized parties [144].

However, if one carefully analyzes the above definitions, there is common ground of understanding and, in fact, strong agreement underlying the written discrepancies between the seemingly incompatible views on availability. To conclude, availability means that information is promptly accessible for only authorized users. Nevertheless, expectations formulated toward availability are far-reaching, borrowing its qualities from non-functional requirements such as capacity, performance, usability and fault tolerance [144]. Yet, in this case, such a broad view hardly helps to conceptualize its concise meaning.

Considering availability in terms of the above-formulated definition, two paradigms come to the fore, namely reliability and access control. While the former can be defined as the probability of a cryptocurrency service (an app) to meet certain performance requirements, the latter can be specified as the means to control privileges or rights to cryptocurrency assets. In practice, availability can be measured by the percentage of the availability of a service (or app) for its users, or even simpler, it can be expressed by the duration of service unavailability in a fixed period of time (e.g., week, month, year), usually termed downtime [145].

Actually, access control is a major part of any system's security [146], typically imperative for these responsible for managing financial assets [147]. The access control is governed by the security policies [148], which precisely define the authorized actions for all users in the scope of a particular wallet, including managing the encryption keys used to digitally sign transactions, and buy and sell cryptocurrencies. However, it should be noted that current access control methods, static by nature, might be inadequate for next-generation systems [149].

Last but not least, apart from its prominent role in information security practice [150], voices of criticism against the CIA model have emerged on multiple occasions [151–154]. Indeed, the orientation of the model is, by design, narrowed to technology, and, as a consequence, its adoption intelligibly leads to the organizational and social aspects of security being overlooked. While the greatest risk involved investing in cryptocurrencies lies within the increasing number of crypto scams on people [155], then the arguments for re-examination and reorientation of the CIA model seem to be rational and eventually convincing.

6. Secure Data Transmission Methods

Blockchain technology is recognized as the dominant technology in the cryptocurrency (and digital currency) world market. Not only the largest, currently leading cryptocurrencies such as Bitcoin and Ethereum are implemented with this technology, but many other popular currencies are also blockchain-based (Litecoin, Deuterium, etc.).

Blockchain technology has been adopted for many different fields in which there is a need to exchange some valuable assets. Most notably, there are blockchain-based solution proposed for smart grids [156,157], healthcare and telemedicine [158], smart insurance [159], vehicular energy networks [160], databases [158,161], cloud computing [162], software-defined networks [163], wireless sensor networks [164], trading energy contracts [165] and livestream video transmissions [166]. Some of these solutions use existing implementations

of public blockchains, such as Bitcoin or Ethereum, and some use their own systems. Most of these systems, however, need to provide some sort of currency exchange mechanism which is highly secure. The security model to be applied for the data transmission of digital currency most often depends on the field in which the currency will be applied. In terms of scope and permission level, blockchains can be divided into three different types [166]:

- public type—a public blockchain that every Internet user can operate with (Bitcoin, Ethereum, Litecoin, Deuterium, etc.),
- private type—a blockchain that is a private property of an organization; there is an actor (administrator) who gives permission to other users to access data in order to operate with the blockchain,
- consortium (federated) type—a field of companies, organizations, individuals, representatives or agents together make the decisions regarding the blockchain network; verification of transactions and blocks is implemented through different centers, which decreases the number of points of failure.

Blockchain was recognized as a disruptive technology by offering data immutability, security, decentralization and transparency [158]. It also ensures data integrity, data ownership, and a trusted data source [158]. The peer-to-peer nature of the transactions in blockchain-based systems bypasses third parties' participation in the process, which eliminates the single-point-of-failure problem [157], could positively affect user anonymity, protecting their privacy [158], and could lead to an overall less expensive system [157].

The hash function used by a blockchain should be one-way (i.e., it is hard to determine the input string from the output hash), and collision-resistant (no two inputs can ever produce the same hash output) [167]. Several different hashing algorithms are used in popular blockchain-based systems, for example [167]:

- Bitcoin uses SHA-256,
- Ethereum uses Keccak256,
- Litecoin uses Scrypt,
- Dogecoin uses Scrypt.

Hashes of blocks are stored in a data structure called a Merkle Tree (or hash tree [162,167], introduced by Ralph C. Merkle [168]. The Merkle Tree is a tree data structure in which hashes of data blocks are stored in leaves, and every non-leaf vertex stores the hash of its children content (hashes). A Merkle Tree is usually implemented as a binary tree (every non-leaf vertex has at most 2 children). The hash stored in a Merkle Tree root (Merkle root) is then stored in the header of a data block, and can be used to verify that the transmitted block is whole, undamaged and unaltered. Public and private key pairs are often generated using the Elliptic Curve Digital Signature Algorithm (ECDSA) or RSA.

There are some reports of security issues that are still present in data transmission in blockchain-based solutions. However, solutions or countermeasures have already been proposed by researchers for many of these challenges in the form of modifications to blockchain algorithms and data structures. Another important issue is collision resistance of cryptographic hash functions [169].

Solutions based on popular public blockchains, such as Bitcoin or Ethereum, are not applicable for transactions with huge volumes of data due to scalability issues, which could be mitigated with technologies such as the InterPlanetary File System [170] and BigChainDB [171]. In public blockchains, there are also problems with user privacy, which can be eliminated by implementing a private or consortium-type of blockchain with a hybrid encryption method, in which the user's data is encrypted with a symmetric password, and afterwards the symmetric password is encrypted with an asymmetric pair of keys [158]. The anonymity of the user can be further secured by implementing Zero Knowledge Proof protocols for authentication [172].

The long distance in kilometers between trading locations is a characteristic feature of the current globalization of transactions. Long transmission distances (often implemented via

satellite transmission systems) can adversely affect the security of real-time transactions [173]. To combat this, several optimizations for hash algorithms have been formulated [173].

It is worth mentioning that digital currencies not based on blockchain often offer significantly faster transaction speeds. For example, Ripple (XRP) confirms its transactions in around 5 s, while it takes approximately 10 min to confirm a transaction in Bitcoin [174]. There are studies and experiments performed to optimize other cryptographic operations in cryptocurrencies as well, including secure key transmission and smart contract execution [175] and the process of cryptocurrency mining [27]. These optimizations not only speed up the process, but often also minimize the amount of energy needed for computations, which is crucial for smart grids [176,177].

Some researchers propose secure validation methods and pricing schemes for blockchain-based peer-to-peer applications with a game theory approach [178]. This idea promotes the idea of rewarding users that are helping with a successful delivery, prevents selfish actions exhibited by users, and prevents their collusion.

To sum up, blockchain technology is commonly used for digital currencies nowadays because of its high level of security. The idea is relatively new, but quite popular among researchers around the world, who are proposing modifications to the original idea to overcome the increasingly many challenges identified (i.e., high energy consumption, long operation times, scalability issues, etc.) and security issues (weaknesses of internally used algorithmic procedures, increased vulnerability to attacks caused by long-distance transmissions, and problems with users' privacy and lack of anonymity, just to name a few).

7. Social Engineering Attacks and Countermeasures

Naturally, the users of cryptocurrencies are at risks of scams and identity theft. In general, social engineering techniques take advantage of deception and manipulation [179]. In place of attacks on software and hardware technologies, social engineers target humans, aiming to compromise private information. In 2022, Hetler specified nine common cryptocurrency scams, namely: Bitcoin investment scheme, employment offers and fraudulent employees, fake cryptocurrency exchanges, man-in-the-middle attack, phishing scams, ponzi schemes, romance scams, rug pull scams, and social media cryptocurrency giveaway scams [180]. They often leads to theft or distortion, data destruction, or fake transactions [181]. Yet, due to their unconventional and sophisticated nature, social engineering attacks (SEAs) are still being heavily investigated [182], in order to better understand their mechanisms of occurrence and scenarios of performance, which is essential to prevent and reduce their negative impact.

7.1. Social Engineering Attacks

By definition, social engineering is "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes" [183]. The social engineering attack (SEA) is defined as an action, where "an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems" [184]. Social engineering is targeting Internet-related systems in particular, and is increasingly being applied to cryptocurrency users [185].

From a user perspective, a security breach involves stealing passwords and wallet private keys in the case of cold (off-line) wallets [186], or obtaining unauthorized access to the user's on-line accounts, including information such as an email address with the password, and phone number linked to the account, as well as access to the associated email account in the case of hot (on-line) wallets [187]. Such an attack can be performed by spreading fake news, which is defined as "purposefully crafted, sensational, emotionally charged, misleading or totally fabricated information that mimics the form of mainstream news" [188].

One can distinguish three categories of SEAs [189]:

- technology-based,
- human-based (social approach),

- hybrid (socio-technical approach).

7.1.1. Technology-Based Attacks

Using technical tactics, the social engineer employs computer applications to trick users into taking a specific action. People-based tactics, on the other hand, are performed by attackers who understand the shortcomings of the human psyche [190].

Hackers use many different techniques to steal a user's sensitive information, and thus, for example, gain unlimited access to their bank account.

- Spyware. Spyware is very difficult to detect. Its task is to discreetly collect and send other people information about the user, such as personal data, payment card numbers, access passwords, addresses of visited websites, interests (which can be inferred from the search queries) and e-mail addresses. Such a program is usually associated with another application, or a file downloaded from a website on the web. Sometimes, it is also attached to e-mail attachments [191,192].
- Adware. These types of programs, also known as adware, are very annoying, but usually not particularly dangerous. They work by displaying pop-up ads both when running other applications and when idle. Similarly to spyware, adware is most often bundled with free programs downloaded from the web [193].
- Keylogger. This software records the keys pressed by the user and thus collects data such as credit card numbers and passwords. Keyloggers also come in the form of small devices attached to the keyboard port [194].
- Ransomware. Ransomware is a much more advanced cyberattack technique, which consists in blocking access to certain files and offering to unblock them for a hefty fee. Of course, hackers rarely keep their promise, even if they receive the ransom. Such a program is typically installed simultaneously with other programs without the user's knowledge while using an unsecured network, infected website, or email attachment [195].
- Trojan. A Trojan (Trojan horse), is a program that imitates a useful application that the user installs on their device. This software gives unauthorized persons access to the computer or telephone. Similarly to other types of viruses, the Trojan can hide in email attachments, illegally downloaded movies, and free applications [196].
- Worm. These types of programs have the ability to replicate and spread by themselves using a computer network. They are usually used for activities such as sending e-mails or destroying files on the disk. Such activities consume the bandwidth of networks and devices, making the latter often become very slow and even stop responding to commands [193].

7.1.2. Human-Based Attacks

Social engineering attacks on cryptocurrency users exploit the human factor [185]. Socially based cyberattacks can appear by employing various acts, such as tailgating, impersonating, eavesdropping, shoulder surfing, dumpster diving, reverse social engineering, and others [197]. Attackers often use the five principles of persuasion: first—authority and power; second—social proof, liking, likeness; third—deception; fourth—commitment, reciprocity and consistency; and fifth—distraction [198].

- Impersonating. Through impersonation, the threatening player assumes a false identity to gain credibility that will enable them to perform malicious acts such as piggybacking, pretexts and quid pro quo.
- Tailgating/piggybacking. Tailgating, another popular social engineering program, involves following someone with authorized access into a building or system and thus using someone else's authorization to gain access to a data source. This is similar to pretending to be someone who has forgotten an ID, supposedly in need of help and playing on the innate human trait of being helpful [199,200]. Tailgating is the act of following the unconscious goal of a person with legal access through a secure door

into a confined space. This can be compared to when the attacker asks the victim to hold the door, or simply walks in before it closes [197].

- Eavesdropping. Eavesdropping is an act of secretly or stealthily extracting information from an interaction in which it is taking no part, including channels such as emails, instant message, videoconference and phone lines [197,201].
- Shoulder surfing. Through shoulder surfing, an attacker directly observes the victim over their shoulder to collect personal information and credentials [197,201].
- Reverse social engineering. The attacker encourages their victim to initiate the interaction. The player lurks, plays the role of a trustworthy character, fabricates a problem for the victim and indirectly presents a real solution. They inspire trust and extort the data they need [197,201].
- Pretexting. Malicious hackers pretend to be someone other than who they are, such as a system operator, to obtain confidential information about a person or company. For example, an attacker calls an employee and asks them to confirm their username and password for security reasons [182,190]. Using a variety of pretexts and deception, a hacker can create a fake website on the Internet (such as a fake bank website) to influence a targeted victim to disclose confidential information to perform an action that poses a threat to themself or their company [202].
- Quid pro quo. The main feature of this type of attack is to give someone something back. The attacker does a good deed for the victim, who may then be more likely to return the favor. The easiest way to prepare for an attack is to search the Internet and gather information about the company. It is also possible to call to obtain specific information and to exploit published vulnerabilities [189,199,203].
- Dumpster Diving. During dumpster diving, attackers search corporate computer trash cans, assuming they will find useful protected information about the company, network, and its employees [185,204]. Dumpster diving is a non-traditional search and is legal and very common, and often provides a wealth of information [205].

7.1.3. Hybrid Attacks

The following types of hybrid attacks have been identified, using social influence techniques (the so-called socio-technical approach):

- Baiting is an example of a social engineering attack based on malware-infected media storage made to appear abandoned in a public place, to be found and used by a future attack victim. For example, a USB device with an appealing label infected with a Trojan horse could be left in a bank location or another place with an increased probability to be found by a targeted victim [206]. Hackers preload malware onto external storage devices (e.g., CDs or USBs) and strategically leave them in generally accessible public areas of the targeted company. When employees pick up the CDs or USBs carrying the malware, they connect them to their computers [190,207].
- Trolling is a form of cyberbullying and harassment on the Internet; its manifestations include, for example, publishing and sending information or videos of public suicide attempts, songs, such as lullabies for children, to which hackers attach malware [207,208]. Trolls manipulate public opinion to spark social discourse and exploit "human bias against binary choices" [209]. The tactics used by trolls to achieve the desired extremes are "lies, evasions, untruths, alternatives, improbable theories, distortions, ad hominem attacks, and other rhetorical measures as part of Machiavellian propaganda or handover campaigns" [209]. Trolling uses phishing attack methods, computers, and network systems to manipulate Internet users' perceptions of information, make them think differently, and motivate them to do something they would not have thought of on their own.
- Phishing is a form of attack in which social engineers send fake email messages that recipients find legitimate. The email may ask you to click on a malicious link or take action that exposes sensitive data [190,210]. A phishing attack is fraudulent activity and a crime that is aimed at acquiring personal information, e.g., personal ID details,

credit card and bank details, such as passwords and phone details, by pretending to be a legitimate entity or person with a pseudo-legitimate purpose [211].

- Pharming attack is a domain name system (DNS)-based phishing attack that relies on tampering with bank host files or DNS [212]. In a DNS-based phishing attack, a hacker redirects the user to a fraudulent website or the hacker's device when the attack victim tries to access a legitimate bank website, in order to obtain a copy of the user's bank credentials [212]. A pharming attack can be performed by a malware installation on the bank user's device or by tampering with the e-bank domain; in any case, when entering the proper bank URLs on the browser, the user is automatically redirected to a fraudulent web page [213].
- Malware attachments Phishing also often contains malware attachments or programs that attackers install on the user's device. Malware-based phishing could take place when the bank user or employee accesses an unauthorized webpage and unintentionally downloads a malicious piece of software [212]. When the user accesses the unauthorized website, a program with a keylogger is automatically downloaded and installed on the user's device, which is then used by the attackers to steal confidential information and the user's bank credentials [214]. Thereafter, the keylogger gathers the user's personal data and credentials in the form of keystroke information, and sends them to the hackers in a file that will later be used by the hackers to commit financial crimes [214].
- Watering Hole is an attack that requires advanced technical knowledge. The attacker identifies one or more legitimate websites regularly visited by the targeted user. The hacker looks for vulnerabilities, infects the most vulnerable website, and waits [197,215].
- Smishing is a combined form of SMS and phishing in which attackers send the victim SMS messages containing malicious content. This content sometimes contains links that redirect the user to websites with malicious applications and user interfaces [216].
- Whaling is a type of attack which specifically targets top management, profiling company goals using highly personalized threat analysis. These forms represent broad categories and there is a need to develop clearer descriptions and details of specific attacks in order to understand their rate of occurrence and their impact on organizations [217].

In summary, cybercriminal activities are currently targeted at cryptocurrencies due to the pseudonymity and privacy they offer. Attackers continue to cause new losses, even as masses of scientists are actively analyzing and developing innovative defense mechanisms to prevent these actions [218]. Thus, the most commonly employed attacks are phishing, smishing, and vishing [219]. Phishing attacks are among the most widespread social engineering attacks and can use complex techniques such as, for example, the "Man in the middle" (MITM) attack [212]. The MITM attack is characterized by hackers placing themselves in the middle of the digital communication chain between the e-bank and its customers, where both the bank and the customer are not aware of the attack, while confidential data and credentials are compromised [220]. Regardless of the chosen attack technique, the hackers aim to gain e-banking users' data and credentials in order to conduct financial frauds and illegally harvest the users' money for the hacker's benefit [212].

7.2. Countermeasures against Cyber Attacks

Regardless of the social engineering method (see Table 1, in order to counter the attack, bank users and staff should regularly complete online security training, be aware of the potential threats and attack techniques, use two-factor authentication, install and upgrade their antivirus software from a legitimate source, and be conscious of the potential threats and suspicious communications/websites they could be exposed to.

Table 1. Common social engineering attacks and countermeasures. Own elaboration based on [213].

Type of attack	Countermeasures
Phishing attack	• Users should precisely inspect URLs and check whether they redirect to new and suspicious web page, whether emails contains hyperlinks and suspicious attachments. • Users should check for spelling mistakes, salutations, pay attention to tones of urgency and emotional intensity of the emails.
Watering Hole Attack	• Users should have security proxy gateways able to defend from opportunistic drive-by downloads, prevent criminal redirection, rootkits and malware from being deployed. • Users should choose email solution which could perform dynamic malware analysis of the emails.
Smishing attack	• Users should avoid unknown and suspicious phone numbers and avoid giving personal information through text-messages. • Users should pay attention to tones of urgency and emotional intensity of the message. • Users should check suspicious links, applications and campaigns independently from sms or call messages.
Vishing attack	• User could ask for the caller's official credentials and check them and the number independently. • Users could avoid answering to unknown and suspicious phone numbers and avoid to give personal information by phone. • User could end suspicions call and call the institution back using known and verified number.
Whaling	• Users should deploy anti-phishing software performing URL screening and link validation. • Users should carefully check the sender email address and credentials. • User's security training is important.
Pharming	• Effective and regularly-updated antivirus software is essential to spot pharming attacks. • Users should log-in and provide their credentials on https websites that are protected. • Users should check security upgrades from a trusted Internet Service Provider.

The owners of cryptocurrencies definitely have to reckon with cyberattacks of various types. However, regardless of the type of attack, the victim's trust, naivety, lack of vigilance, lack of knowledge, unbelief in the possibility of an attack, or some thoughtlessness may be to their detriment.

8. Discussion

In recent years, researchers have developed various methods to counter phishing. However, the problem still exists [221]. Many users do not take cyberattacks seriously. Cybercrime should be treated the same as any other type of crime, and make it not pay for hackers to attack. Typically, in the case of a cyberattack, everyone focuses on blaming the victims instead of prosecuting the perpetrators. Instead, the companies attacked are treated as the culprits. At the same time, it is accepted that criminals escape punishment due to the lack of a globally agreed legal framework and an adequate justice system [222]. Internet users are reasonably aware of cyber threats but use only minimal protective measures that are usually relatively common and straightforward. Higher cyber awareness depends on a person's level of cyber-education, competence and knowledge [223] and on the user's country and the country's educational conditions [224] as well as their gender [225]. Awareness is also related to the use of protection tools but not to the information that IT users were willing to disclose [226].

In information security research, personality traits are considered primary predictors of human behavior. For example, the so-called Big Five Model identifies five components of personality: agreeableness, conscientiousness, extraversion, openness, and stress tolerance. A user's confidence, competence, motivation, and previous experience with cybercrime are essential in explaining the impact of the Big Five personality traits on vulnerability to cyberattacks in social network settings [227]. Conscientiousness, agreeableness, and neuroticism strongly reduce users' vulnerability to cyberattacks in social network settings. While extraversion turns out to significantly increase a user's likelihood of falling victim to cyberattacks [228].

Personality is the most critical factor affecting, for instance, the susceptibility to phishing. Despite having knowledge and experience, when people encounter something new, their personality strongly influences their behavior. The second most crucial factor is cognitive processing, which shows how a person processes information and affects whether they click on links; some people are more cautious, while others are more casual. The third most important factor is computer knowledge, which can help people better distinguish between phishing and legitimate e-mails [229,230].

Influential cybersecurity professionals who can defend themselves against cyberattacks differ from other employees, even standard information technology professionals, on trust, intellect, sympathy, vulnerability, self-consciousness, assertiveness, and adventure at the trait level [231]. Cybersecurity professionals score significantly lower than other employees in agreeableness, openness, and trust [231,232].

Given the need for cybersecurity specialists to protect their companies and loved ones from outside threats, it is understandable that they may be less trusting of individuals, as anyone can access a computer and pose a threat. Cybersecurity specialists scored higher than other employees on intellect. High correlations were found between information technology specialists and openness, but because intellect is derived from openness, cybersecurity specialists were already inclined to score relatively high on this trait [231,232].

Companies paying ransoms to recover data are signaling to cybercriminals that ransomware attacks are a way to make easy money and encouraging them to continue their criminal activities [233]. Once victims stop paying, ransomware attacks will become less frequent as they lose effectiveness [234]. Even though companies affected by cybercrime are victims, they should protect any data they use, process, and store [235]. Paying cybercriminals to restore access to systems cannot be considered a defense strategy [236], since it does not work in the long run [237].

Building a cybersecurity culture framework with a clear focus on the human factor is essential, which can help detect possible threats from both malicious and unintentional insiders [238]. While the law does not fully protect us from cybercrime, primal human survival instinct tells us that we should defend ourselves [239]. This requires taking a few basic steps. First, every company should employ a dedicated IT security manager, working on-site, with regular contact with company management and the authorities to take security initiatives. Smaller companies also need a person in charge of cyber security who specializes in data protection.

Second, companies must observe digital hygiene. This includes, in particular, mandatory training for all employees so they can detect potential attacks, know whom to report them to, and understand why this is so important. The more employees are involved in implementing digital hygiene, the more aware they will be of the risks and the more effectively they will prevent them [240].

Third, both individuals and teams should receive coaching and training that can strengthen not only their hard competencies in cyber defense. We also suggest the development of individual dispositions and soft competencies in terms of calculated trust and caution, especially to proposals for so-called big wins, conducting business and phishing.

Summing up, such factors as technical and programmatic safeguards at the organization level, team education on cyberattacks and how to defend against them, and individual education and competence development in knowledge, skills, soft dispositions and social skills to defend against cyberattacks can lead to the effective defense against cyberattacks, and stability for the organization.

8.1. Theoretical Implications

The theoretical implications of our research are the opportunities to develop conceptual and empirical models based on the issues classified, defined, and analyzed. Our paper provides a theoretical basis for a broad discourse on resistance to the cyber security of digital currencies from both technical and human-oriented perspectives.

8.2. Practical Implications

Our research not only contributes to the theory but also provides important practical implications. Our findings can serve as a warning to individual Internet users, as well as companies, organizations, and even local and central governments on how to secure their information systems against cyberattacks. We placed special emphasis on aspects that take into account cryptocurrencies, which, to the best of our knowledge, might become the basis for the exchange of goods and services in the near future.

8.3. Study Contributions

Our contribution is a broad critical literature review, the discussion on the background of the development of cryptocurrencies, the review of crypto wallet definitions and classification, the analysis of security architectures with the description and exemplification of the related models. Moreover, we recognized and localized the data transmission methods developed for blockchain-based solutions. Furthermore, we elaborated on the adopted social engineering attacks and adapted countermeasures for cryptocurrencies. Finally, we concluded the paper with the theoretical and practical implementations of the performed study.

8.4. Study Limitations

The limitation of our study is that it is only a critical analysis of the literature, it does not constitute an empirical study based, for example, on questionnaires among Internet users. We will address this problem with experimental research in the future, where we intend to target two groups of Internet users: those who have been the victim of a cyberattack and have suffered heavy losses as a result, and those who have been able to resist cyberattacks. We also want to test the psychological characteristics of these two

groups of people using the relevant tools, to better suggest to users what qualities they need to develop in themselves in order not to succumb to cyberattacks. We also want to indicate how to effectively defend against cyberattacks from both the technical and cyber perspectives.

9. Conclusions

In this study, we have analyzed and reviewed the recent literature on the security of cryptocurrencies, in particular focusing on the both technology-oriented solutions and human-related factors. It seems that neither the former is robust enough nor latter is mature enough to conclude that security issues are no longer present. In fact, on the contrary, a recent report from Trail of Bits provides examples of how immutability of distributed ledger technology (DLT) can be broken by subverting the properties of a blockchain's implementations, networking, and consensus protocol [241]. On the other hand, people are still the weakest link in the security chain and are chronically responsible for 95% of failures of security systems [242]. Considering the possible countermeasures to implement, obviously one concerns human factor and involves users' education and training, whereas the opposite relies on the software systems and tools, recently also armed with artificial intelligence-based defense techniques [243].

Nevertheless, the success of cryptocurrencies has brought the attention of governments and central banks. According to the International Monetary Fund (IMF), the interest in exploring the possibilities of launching a central bank digital currency (CBDC) is a matter of the highest urgency [244]. At the moment, 105 countries, representing over 95 percent of global GDP, are exploring a CBDC, while 50 countries are in an advanced phase of exploration (development, pilot, or launch) [245]. In particular, 19 countries from the G20 (Group of Twenty) are considering issuing CBDCs, and the majority are beyond the research stage. Therefore, concerns about cybersecurity and privacy are now matters of state.

At the moment, there are three main varieties of digital currency, namely: cryptocurrency, stablecoins and central bank digital currency. In this realm, security is still a major tenet, including protection against double-spending, counterfeiting, and account and data breaches [246], just to name a few. Undeniably, the desire to come to grips with cybersecurity risks and to be able to find a fair balance for all interested parties has become an area of interest both academically and commercially in recent years, primarily as a consequence of the ongoing revolution [247].

Undoubtedly, new payment systems, with recent technological advancements, will benefit both businesses and individuals in the areas of trust, regulatory stability, and audit transparency [248]. Moreover, the systematic development of users' security awareness, achieved through education, training and testing, will also provide proactive measures to mitigate the risks and threats. Having said that, in our opinion, future research should pay more attention to elaborating proactive cybersecurity risk mitigation strategies, covering prevention, detection and remediation issues.

Author Contributions: Conceptualization, P.W.; Methodology, P.W.; Investigation, P.W.; Writing—original draft, P.W., K.W., H.A. and J.K.; Writing—review & editing, P.W.; Supervision, P.W.; Project administration, P.W. All authors have read and agreed to the published version of the manuscript.

Funding: The Greencoin project has received funding from the "Applied Research—Cities for the future: services and solutions" program (under grant agreement no. NOR/IdeaLab/GC/0003/2020-00). The project benefits from a 1.9 million euro grant from Iceland, Liechtenstein and Norway through the EEA Grants. The National Centre for Research and Development is the project Operator. The project is co-financed at the level of 15% from Polish budgetary funds.

Data Availability Statement: Not applicable.

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

References

1. Weinberg, C.B.; Otten, C.; Orbach, B.; McKenzie, J.; Gil, R.; Chisholm, D.C.; Basuroy, S. Technological change and managerial challenges in the movie theater industry. *J. Cult. Econ.* **2021**, *45*, 239–262. [CrossRef]
2. Mamatzhonovich, O.D.; Khamidovich, O.M.; Esonali o'g'li, M.Y. Digital Economy: Essence, Features and Stages of Development. *Acad. Globe: Inderscience Res.* **2022**, *3*, 355–359.
3. Hodson, R. Digital Revolution. *Nature* **2018**, *563*, S131. [CrossRef]
4. Hitpass, B.; Astudillo, H. Industry 4.0 challenges for business process management and electronic-commerce. *J. Theor. Appl. Electron. Commer. Res.* **2019**, *14*, I–III. [CrossRef]
5. Palos-Sanchez, P.R.; Correia, M.B. The collaborative economy based analysis of demand: Study of Airbnb case in Spain and Portugal. *J. Theor. Appl. Electron. Commer. Res.* **2018**, *13*, 85–98. [CrossRef]
6. Rot, A.; Sobińska, M.; Hernes, M.; Franczyk, B. Digital transformation of public administration through blockchain technology. In *Towards Industry 4.0—Current Challenges in Information Systems*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 111–126.
7. Reiff, N. What Are the Advantages of Paying with Bitcoin? 2021. Available online: https://www.investopedia.com/ask/answers/100314/what-are-advantagespaying-bitcoin.asp (accessed on 19 August 2022).
8. Salman, A.; Razzaq, M.G.A. *Blockchain and Cryptocurrencies*; IntechOpen: London, UK, 2019.
9. Achim, M.V. A Cryptocurrency Spectrum Short Analysis. *J. Risk Financial Manag.* **2020**, *13*, 227.
10. deRitis, C. *Digital Currencies: Risks and Opportunities*; GARP: Jersey City, NJ, USA, 2021.
11. McMillan, R. The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster. 2021. Available online: https://www.wired.com/2014/03/bitcoin-exchange/ (accessed on 19 August 2022)
12. Copeland, T. 7 Most-Damaging Bitcoin Scams and Hacks of all Time. 2021. Available online: https://decrypt.co/6236/biggest-hacks-and-scams-in-bitcoin-history (accessed on 19 August 2022)
13. *ISO/IEC 27032:2012*; Information Technology—Security Techniques—Guidelines for Cybersecurity. ISO: Geneva, Switzerland, 2012.
14. Dai, F.; Shi, Y.; Meng, N.; Wei, L.; Ye, Z. From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In Proceedings of the 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, China, 11–13 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 975–979.
15. Hasanova, H.; Baek, U.J.; Shin, M.G.; Cho, K.; Kim, M.S. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *Int. J. Netw. Manag.* **2019**, *29*, e2060. [CrossRef]
16. Demirkan, S.; Demirkan, I.; McKee, A. Blockchain technology in the future of business cyber security and accounting. *J. Manag. Anal.* **2020**, *7*, 189–208. [CrossRef]
17. Glaser, B.G.; Strauss, A.L.; Strutzel, E. The discovery of grounded theory; strategies for qualitative research. *Nurs. Res.* **1968**, *17*, 364. [CrossRef]
18. Amer, A. *Analytical Thinking*; Pathways to Higher Education; Cairo University: Giza, Egypt, 2005.
19. Rapley, T. Sampling strategies in qualitative research. In *The SAGE Handbook of Qualitative Data Analysis*; Sage: Newcastle, UK, 2014; pp. 49–63.
20. Heartfield, R.; Loukas, G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Comput. Secur.* **2018**, *76*, 101–127. [CrossRef]
21. Charmaz, K. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*; Sage: Newcastle, UK, 2006.
22. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Keele, UK, 2007.
23. Google. Search Query Language. 2020. Available online: https://developers.google.com/issue-tracker/concepts/search-query-language (accessed on 19 August 2022)
24. Merriam-Webster Dictionary. *Cryptocurrency*, 2021.
25. Cambridge Dictionary. *Cryptocurrency*, 2021.
26. Kim, H.; Jang, J.; Park, S.; Lee, H.N. Error-correction code proof-of-work on Ethereum. *IEEE Access* **2021**, *9*, 135942–135952. [CrossRef]
27. Alkaeed, M.K.; Alamro, Z.; Al-Ali, M.S.; Al-Mohammed, H.A.; Khan, K.M. Highlight on Cryptocurrencies Mining with CPUs and GPUs and their Benefits Based on their Characteristics. In Proceedings of the 2020 IEEE 10th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 9 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 67–72.
28. Jian, M.S.; Pan, C.J. Blockchained industry information handoff based on internet of things devices with intelligent customized object recognition. *Sensors* **2022**, *22*, 2312. [CrossRef] [PubMed]
29. Gundaboina, L.; Badotra, S.; Bhatia, T.K.; Sharma, K.; Mehmood, G.; Fayaz, M.; Khan, I.U. Mining cryptocurrency-based security using renewable energy as source. *Secur. Commun. Netw.* **2022**, *2022*, *4808703*. [CrossRef]
30. Szmigielski, A. *Bitcoin Essentials*; Packt Publishing Ltd.: Birmingham, UK, 2016.
31. Wang, Z. Security and privacy issues within the Cloud Computing. In Proceedings of the 2011 International Conference on Computational and Information Sciences, Chengdu, China, 21–23 October 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 175–178.
32. Chohan, U.W. A History of Bitcoin. 2017. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875 (accessed on 19 August 2022).
33. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260.

34. Greenberg, A. Nakamoto's Neighbor: My Hunt for Bitcoin's Creator Led to a Paralyzed Crypto Genius. 2014. Available online: https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/?sh=1207c9134a37 (accessed on 19 August 2022).
35. Cvllr, J. The Value Overflow Incident in the Bitcoin Blockchain—15th August 2010. 2018. Available online: https://jeancvllr.medium.com/the-value-overflow-incident-in-the-bitcoin-blockchain-15th-august-2010-a59a516e03db (accessed on 19 August 2022).
36. Shrem, C. Bitcoin's Biggest Hack in History: 184.4 Billion Bitcoin from Thin Air. 2019. Available online: https://hackernoon.com/bitcoins-biggest-hack-in-history-184-4-ded46310d4ef (accessed on 19 August 2022).
37. CNBC. Everything You Need to Know about the Blockchain. 2018. Available online: https://www.cnbc.com/2018/06/18/blockchain-what-is-it-and-how-does-it-work.html (accessed on 1 December 2022).
38. Hayes, A. What Happens to Bitcoin after All 21 Million Are Mined? 2021. Available online: https://www.nasdaq.com/articles/what-happens-when-all-21-million-bitcoin-are-mined (accessed on 2 December 2022).
39. Chang, T.H.; Svetinovic, D. Data analysis of digital currency networks: Namecoin case study. In Proceedings of the 2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS), Dubai, United Arab Emirates, 6–8 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 122–125.
40. Hitam, N.A.; Ismail, A.R. Comparative performance of machine learning algorithms for cryptocurrency forecasting. *Ind. J. Electr. Eng. Comput. Sci.* **2018**, *11*, 1121–1128. [CrossRef]
41. Statista. Number of Cryptocurrencies Worldwide from 2013 to November 2021. 2021. Available online: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/ (accessed on 14 October 2022).
42. CoinMarketCap. Total Cryptocurrency Market Capitalization (Excluding Bitcoin). 2021. Available online: https://www.globaldata.com/data-insights/financial-services/bitcoins-market-capitalization-history/#:~:text=Bitcoin%20(BTC)%20had%20the%20highest,coins%20or%20tokens%20in%20circulation (accessed on 15 October 2022).
43. Tretina, K.; Adams, M. Top 10 Cryptocurrencies of 2023. 2023. Available online: https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/ (accessed on 19 August 2022).
44. *ISO/IEC 27040:2015*; Information Technology—Security techniques—Storage Security; ISO: Geneva, Switzerland, 2015.
45. Techopedia. Security Breach. 2017. Available online: https://www.techopedia.com/definition/29060/security-breach (accessed on 19 August 2022).
46. Gebel, M. Misinformation vs. Disinformation: What to Know about Each Form of False Information, and How to Spot Them Online. 2021. Available online: https://www.businessinsider.com/guides/tech/misinformation-vs-disinformation (accessed on 1 December 2022).
47. IGI Global Dictionary. What is Fraud. Available online: https://www.igi-global.com/dictionary/forensic-accounting-and-corporate-governance/11506#:~:text=An%20intentional%20act%20of%20deceiving,and%20Investigation%20in%20Digital%20Environment (accessed on 19 August 2022).
48. Robertson, H. The Estimated Number of Global Crypto Users Has Passed 100 Million—And Boomers Are Now Getting Drawn to Bitcoin Too, Reports Find. 2021. Available online: https://www.businessinsider.in/stock-market/news/the-estimated-number-of-global-crypto-users-has-passed-100-million-and-boomers-are-now-getting-drawn-to-bitcoin-too-reports-find/articleshow/81210262.cms (accessed on 23 July 2022).
49. Reinicke, C. 1 in 10 People Currently Invest in Cryptocurrencies, Many for Ease of Trading, CNBC Survey Finds. 2021. Available online: https://www.cnbc.com/2021/08/24/1-in-10-people-invest-in-cryptocurrencies-many-for-ease-of-trading.html (accessed on 24 July 2022).
50. Oh, H.; Nam, K.; Jeon, S.; Cho, Y.; Paek, Y. MeetGo: A Trusted Execution Environment for Remote Applications on FPGA. *IEEE Access* **2021**, *9*, 51313–51324. [CrossRef]
51. Karantias, K. SoK: A Taxonomy of Cryptocurrency Wallets. *IACR Cryptol. ePrint Arch.* **2020**, *2020*, 868.
52. Li, C.; He, D.; Li, S.; Zhu, S.; Chan, S.; Cheng, Y. Android-based Cryptocurrency Wallets: Attacks and Countermeasures. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Virtual, 2–6 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 9–16.
53. He, D.; Li, S.; Li, C.; Zhu, S.; Chan, S.; Min, W.; Guizani, N. Security analysis of cryptocurrency wallets in android-based applications. *IEEE Netw.* **2020**, *34*, 114–119. [CrossRef]
54. Kavanagh, C. Custodial vs. Non-Custodial Crypto Wallets. 2021. Available online: https://www.coolwallet.io/custodial-vs-non-custodial-crypto-wallets-whats-the-difference/ (accessed on 15 March 2022).
55. Fröhlich, M.; Wagenhaus, M.R.; Schmidt, A.; Alt, F. Don't Stop Me Now! Exploring Challenges of First-Time Cryptocurrency Users. In Proceedings of the Designing Interactive Systems Conference 2021, Virtual, 28 June 2021–2 July 2021; pp. 138–148.
56. Ozsubasi, I.A. Non-Custodial Wallets Enable Private, P2P Crypto Trading in 2021. 2021. Available online: https://research.aimultiple.com/non-custodial-wallet/ (accessed on 19 August 2022).
57. Suratkar, S.; Shirole, M.; Bhirud, S. Cryptocurrency Wallet: A Review. In Proceedings of the 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 22–23 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–7.
58. Vyas, C.A.; Lunagaria, M. Security concerns and issues for bitcoin. *Int. J. Comput. Appl.* **2014**, 10–12.

59. Moniruzzaman, M.; Chowdhury, F.; Ferdous, M.S. Examining usability issues in blockchain-based cryptocurrency wallets. In Proceedings of the International Conference on Cyber Security and Computer Science, Dhaka, Bangladesh, 15–16 February 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 631–643.
60. Azman, M.; Sharma, K. HCH DEX: A Secure Cryptocurrency e-Wallet & Exchange System with Two-way Authentication. In Proceedings of the 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 305–310.
61. Khan, A.G.; Zahid, A.H.; Hussain, M.; Riaz, U. Security of cryptocurrency using hardware wallet and qr code. In Proceedings of the 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 1–2 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
62. Ojengbede, D. Xpedition Week 5: All About Wallets. 2021. Available online: https://medium.com/mexcglobal/xpedition-week-5-all-about-wallets-e5b235db606c (accessed on 19 September 2022).
63. Cryptopedia. How To Make a Paper Wallet. 2021.
64. Srinivas, R. How to Safeguard Your Cryptocurrency Wallet from Digital Exploits. 2020.
65. Praitheeshan, P.; Xin, Y.W.; Pan, L.; Doss, R. Attainable hacks on Keystore files in Ethereum wallets—A systematic analysis. In Proceedings of the International Conference on Future Network Systems and Security, Paris, France, 1–2 July 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 99–117.
66. Connolly, L.Y.; Wall, D.S. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Comput. Secur.* **2019**, *87*, 101568. [CrossRef]
67. Härtig, H. Security architectures revisited. In Proceedings of the 10th workshop on ACM SIGOPS European Workshop, Saint-Emilion, France, 1 July 2002; pp. 16–23.
68. Conrad, E.; Misenar, S.; Feldman, J. Chapter 6—Domain 6: Security Architecture and Design. In *Eleventh Hour CISSP*, 2nd ed.; Conrad, E., Misenar, S., Feldman, J., Eds.; Syngress: Boston, MA, USA, 2014; pp. 95–116. [CrossRef]
69. Amer, S.H.; Hamilton, J.A., Jr. Understanding security architecture. In Proceedings of the 2008 Spring Simulation Multiconference, Virginia Beach, VA, USA, 23–26 April 2008; pp. 335–342.
70. Tricomi, G.; Scaffidi, C.; Merlino, G.; Longo, F.; Puliafito, A.; Distefano, S. A Resilient Fire Protection System for Software-Defined Factories. *IEEE Internet Things J.* **2021**, *10*, 3151–3164. [CrossRef]
71. Jain, S.; Felten, E.; Goldfeder, S. Determining an optimal threshold on the online reserves of a bitcoin exchange. *J. Cybersecur.* **2018**, *4*, tyy003. [CrossRef]
72. Roth, N. An architectural assessment of bitcoin using the systems modeling language. *Procedia Comput. Sci.* **2015**, *44*, 527–536. [CrossRef]
73. Sedgwick, K. The Hype Has Faded But Demand Remains for Enterprise Blockchains. 2019. Available online: https://news.bitcoin.com/the-hype-has-faded-but-demand-remains-for-enterprise-blockchains/ (accessed on 19 June 2022).
74. IBM. What Is Blockchain Technology? Available online: https://www.ibm.com/topics/blockchain (accessed on 20 June 2022).
75. Zhang, T.; Huang, Z. Blockchain and central bank digital currency. *ICT Express* **2022**, *8*, 264–270. [CrossRef]
76. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in agriculture traceability systems: A review. *Appl. Sci.* **2020**, *10*, 4113. [CrossRef]
77. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
78. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-based applications in education: A systematic review. *Appl. Sci.* **2019**, *9*, 2400. [CrossRef]
79. Bansal, P.; Panchal, R.; Bassi, S.; Kumar, A. Blockchain for cybersecurity: A comprehensive survey. In Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 10–12 April 2020; pp. 260–265. [CrossRef]
80. Paul, A.; Qu, X.; Wen, Z. Blockchain—A promising solution to internet of things: A comprehensive analysis, opportunities, challenges and future research issues. *Peer-Peer Netw. Appl.* **2021**, *14*, 2926–2951. [CrossRef]
81. Du, M.; Ma, X.; Zhang, Z.; Wang, X.; Chen, Q. A review on consensus algorithm of blockchain. In Procedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; Volume 2017, pp. 2567–2572. [CrossRef]
82. Tanana, D. Avalanche blockchain protocol for distributed computing security. In Proceedings of the 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sochi, Russia, 3–6 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–3.
83. Krause, S.K.; Natarajan, H.; Gradstein, L.H. *Distributed Ledger Technology (DLT) and Blockchain*; World Bank Group: Washington, DC, USA, 2017.
84. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. *Sensors* **2020**, *20*, 483. [CrossRef]
85. Górski, T. Continuous delivery of blockchain distributed applications. *Sensors* **2021**, *22*, 128. [CrossRef] [PubMed]
86. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors* **2018**, *18*, 162. [CrossRef] [PubMed]

87. Soltani, R.; Zaman, M.; Joshi, R.; Sampalli, S. Distributed Ledger Technologies and Their Applications: A Review. *Appl. Sci.* **2022**, *12*, 7898. [CrossRef]
88. Valdeolmillos, D.; Mezquita, Y.; González-Briones, A.; Prieto, J.; Corchado, J.M. Blockchain technology: A review of the current challenges of cryptocurrency. In Proceedings of the Blockchain and Applications: International Congress, Ávila, Spain, 26–28 June 2019; Springer: Berlin/Heidelberg, Germany, 2020; pp. 153–160.
89. Long, S.; Basu, S.; Sirer, E.G. Measuring miner decentralization in proof-of-work blockchains. *arXiv* **2022**, arXiv:2203.16058.
90. Garriga, M.; Dalla Palma, S.; Arias, M.; De Renzis, A.; Pareschi, R.; Andrew Tamburri, D. Blockchain and cryptocurrencies: A classification and comparison of architecture drivers. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e5992. [CrossRef]
91. Karantias, K.; Kiayias, A.; Zindros, D. Proof-of-burn. In Proceedings of the Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, 10–14 February 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 523–540.
92. Lee, J.Y. A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Bus. Horiz.* **2019**, *62*, 773–784. [CrossRef]
93. Trump, B.D.; Florin, M.V.; Matthews, H.S.; Sicker, D.; Linkov, I. Governing the use of blockchain and distributed ledger technologies: not one-size-fits-all. *IEEE Eng. Manag. Rev.* **2018**, *46*, 56–62. [CrossRef]
94. O'Leary, D.E. Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intell. Syst. Account. Financ. Manag.* **2017**, *24*, 138–147. [CrossRef]
95. Irresberger, F.; John, K.; Mueller, P.; Saleh, F. The public blockchain ecosystem: An empirical analysis. *NYU Stern Sch. Bus.* **2021**. [CrossRef]
96. Lai, R.; Chuen, D.L.K. Blockchain–from public to private. In *Handbook of Blockchain, Digital Finance, and Inclusion*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 2, pp. 145–177.
97. Fan, S.; Zhang, H.; Zeng, Y.; Cai, W. Hybrid blockchain-based resource trading system for federated learning in edge computing. *IEEE Internet Things J.* **2020**, *8*, 2252–2264. [CrossRef]
98. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
99. Liu, M.; Shang, J.; Liu, P.; Shi, Y.; Wang, M. VideoChain: Trusted Video Surveillance Based on Blockchain for Campus. In *Cloud Computing and Security*; Springer: Cham, Switzerland, 2018; Volume 11066 LNCS, pp. 48–58. [CrossRef]
100. Yamada, Y.; Nakajima, T.; Sakamoto, M. Blockchain-LI: A study on implementing activity-based micro-pricing using cryptocurrency technologies. In Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media, Singapore, 28–30 November 2016; pp. 203–207. [CrossRef]
101. Kairaldeen, A.R.; Abdullah, N.F.; Abu-Samah, A.; Nordin, R. Peer-to-Peer User Identity Verification Time Optimization in IoT Blockchain Network. *Sensors* **2023**, *23*, 2106. [CrossRef]
102. Sompolinsky, Y.; Zohar, A. Secure high-rate transaction processing in bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, Juan, Puerto Rico, 26–30 January 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 507–527.
103. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 557–564.
104. Maurer, F.K.; Neudecker, T.; Florian, M. Anonymous CoinJoin transactions with arbitrary values. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 1–4 August 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 522–529.
105. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous distributed e-cash from bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 19–22 May 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 397–411.
106. Sasson, E.B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Washington, DC, USA, 18–21 May 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 459–474.
107. Rerup, N.; Aslaner, M. *Hands-on Cybersecurity for Architects: Plan and Design Robust Security Architectures*; Packt Publishing Ltd.: Birmingham, UK, 2018.
108. Sancho Larraz, J. Desing and Evaluation of Novel Authentication, Authorization and Border Protection Mechanisms for Modern Information Security Architectures. Ph.D. Thesis, Zaragoza University, Zaragoza, Spain, 2021.
109. Zhang, J.; Tian, R.; Cao, Y.; Yuan, X.; Yu, Z.; Yan, X.; Zhang, X. A hybrid model for central bank digital currency based on blockchain. *IEEE Access* **2021**, *9*, 53589–53601. [CrossRef]
110. Petratos, P.N.; Ljepava, N.; Salman, A. Blockchain technology, sustainability and business: A literature review and the case of Dubai and UAE. In *Sustainable Development and Social Responsibility—Volume 1, Proceedings of the 2nd American University in the Emirates International Research Conference, AUEIRC'18–Dubai, United Arab Emirates, 13 November 2018*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 87–93.
111. Allen, S.; Čapkun, S.; Eyal, I.; Fanti, G.; Ford, B.A.; Grimmelmann, J.; Juels, A.; Kostiainen, K.; Meiklejohn, S.; Miller, A.; et al. *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations*; Technical Report; National Bureau of Economic Research: Cambridge, MA, USA, 2020.

112. Charles, S.; Mishra, P. Reconfigurable network-on-chip security architecture. *ACM Trans. Des. Autom. Electron. Syst. (Todaes)* **2020**, *25*, 1–25. [CrossRef]
113. Gogniat, G.; Wolf, T.; Burleson, W. Reconfigurable security support for embedded systems. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Washington, DC, USA, 4–7 January 2006; IEEE: Piscataway, NJ, USA, 2006; Volume 10, p. 250a.
114. Molina Zarca, A.; Bernal Bernabe, J.; Farris, I.; Khettab, Y.; Taleb, T.; Skarmeta, A. Enhancing IoT security through network softwarization and virtual security appliances. *Int. J. Netw. Manag.* **2018**, *28*, e2038. [CrossRef]
115. Landwehr, C.E.; Heitmeyer, C.L.; McLean, J. A security model for military message systems. *ACM Trans. Comput. Syst. (Tocs)* **1984**, *2*, 198–222. [CrossRef]
116. McLean, J. Security models. *Encycl. Softw. Eng.* **1994**, *2*, 1136–1145.
117. Agarwal, A.; Agarwal, A. The security risks associated with cloud computing. *Int. J. Comput. Appl. Eng. Sci.* **2011**, *1*, 257–259.
118. LogSign. What Is the CIA Triad and Why Is It Important for Cybersecurity? 2018. Available online: https://www.logsign.com/blog/what-is-the-cia-triad-and-why-is-it-important-for-cybersecurity/ (accessed on 16 November 2022).
119. Oxford Reference. Confidentiality. 2021. Available online: https://www.oxfordreference.com/display/10.1093/acref/9780191844386.001.0001/acref-9780191844386-e-875;jsessionid=9670B7E8E53BBA36B1BFDD55DACA0DD9 (accessed on 22 November 2022).
120. Dictionary.com. Privacy. 2021. Available online: https://www.dictionary.com/browse/privacy (accessed on 12 March 2022).
121. Merriam-Webster. Secrecy. 2021. Available online: https://www.merriam-webster.com/dictionary/secrecy (accessed on 19 August 2022).
122. Kulkarni, D.; Ciric, D.; Zulkarnain, F.; Ilica, J. iPass: An Integrated Framework for Educating, Monitoring and Enforcing Password Policies for Online Services. In Proceedings of the SEKE, Citeseer, Boston, MA, USA, 1–3 July 2009; pp. 548–551.
123. Talamantes, J. 4 Key Cryptocurrency Security Measures: Are You Following Them? 2021. Available online: https://www.redteamsecure.com/blog/4-key-cryptocurrency-security-measures-are-you-following-them (accessed on 29 March 2022).
124. Freeman Law. Cryptocurrency Transactions Multi Signature Arrangements Explained. 2021. Available online: https://freemanlaw.com/cryptocurrency-transactions-multi-signature-arrangements-explained/ (accessed on 19 August 2022).
125. Frawley, K.; Miller, D.W.; Miller, C. State of Security Features for Medical Information. In *Information Technology for the Practicing Physician*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 247–253.
126. Haegemans, T.; Snoeck, M.; Lemahieu, W. Towards a precise definition of data accuracy and a justification for its measure. In Proceedings of the International Conference on Information Quality, MIT Information Quality (MITIQ) Program, Ciudad Real, Spain, 22–23 June 2016; p. 16.
127. Cappi, C.; Chapdelaine, C.; Gardes, L.; Jenn, E.; Lefevre, B.; Picard, S.; Soumarmon, T. Dataset Definition Standard (DDS). *arXiv* **2021**, arXiv:2101.03020.
128. Staff Writer. What Is Data Consistency? 2021. Available online: https://www.igi-global.com/dictionary/data-security-issues-and-solutions-in-cloud-computing/6703 (accessed on 5 May 2022).
129. Zikratov, I.; Kuzmin, A.; Akimenko, V.; Niculichev, V.; Yalansky, L. Ensuring data integrity using blockchain technology. In Proceedings of the 2017 20th Conference of Open Innovations Association (FRUCT), Saint-Petersburg, Russia, 3–7 April 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 534–539.
130. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid: Towards sustainable local energy markets. *Comput.-Sci.-Res. Dev.* **2018**, *33*, 207–214. [CrossRef]
131. World Economic Forum. *Data Integrity*; World Economic Forum: Geneva, Switzerland, 2021.
132. Gangadevi, K.; Devi, R.R. A survey on data integrity verification schemes using blockchain technology in Cloud Computing Environment. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Tangerang, Indonesia, 18–20 November 2021; Volume 1110, p. 012011.
133. Platt, M.; Hasselgren, A.; Román-Belmonte, J.M.; De Oliveira, M.T.; De la Corte-Rodríguez, H.; Olabarriaga, S.D.; Rodríguez-Merchán, E.C.; Mackey, T.K. Test, Trace, and Put on the Blockchain? A Viewpoint Evaluating the Use of Decentralized Systems for Algorithmic Contact Tracing to Combat a Global Pandemic. *JMIR Public Health Surveill.* **2021**, *7*, e26460. [CrossRef]
134. Wagner, K.; Némethi, B.; Renieris, E.; Lang, P.; Brunet, E.; Holst, E. Self-Sovereign Identity. A Position Paper on Blockchain Enabled Identity and the Road Ahead. 2018. Available online: https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf (accessed on 15 May 2022).
135. Aftab, M.U.; Qin, Z.; Hundera, N.W.; Ariyo, O.; Son, N.T.; Dinh, T.V. Permission-based separation of duty in dynamic role-based access control model. *Symmetry* **2019**, *11*, 669. [CrossRef]
136. Plachkinova, M.; Knapp, K. Least Privilege across People, Process, and Technology: Endpoint Security Framework. *J. Comput. Inf. Syst.* **2022**, 1–13. [CrossRef]
137. Popchev, I.; Radeva, I.; Velichkova, V. The impact of blockchain on internal audit. In Proceedings of the 2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE), Sofia, Bulgaria, 29–29 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–8.
138. Gomaa, A.A.; Gomaa, M.I.; Stampone, A. A transaction on the blockchain: An AIS perspective, intro case to explain transactions on the ERP and the role of the internal and external auditor. *J. Emerg. Technol. Account.* **2019**, *16*, 47–64. [CrossRef]
139. Merriam-Webster Dictionary. Availability. 2021. Available online: https://www.merriam-webster.com/dictionary/availability (accessed on 19 August 2022).

140. Merriam-Webster Dictionary. Available. 2021. Available online: https://www.merriam-webster.com/dictionary/available (accessed on 19 August 2022).
141. Qadir, S.; Quadri, S. Information availability: An insight into the most important attribute of information security. *J. Inf. Secur.* **2016**, *7*, 185–194. [CrossRef]
142. Office for Official Publications of the European Communities. *Information Technology Security Evaluation Criteria (ITSEC)*; Technical Report; Publications Office of the European Union: Luxembourg, 1991.
143. National Institute of Standards and Technology. Federal Information Security Modernization Act (FISMA). 2014. Available online: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act (accessed on 23 May 2022).
144. Pfleeger, C.P.; Pfleeger, S.L. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*; Prentice Hall Professional: Upper Saddle River, NJ, USA, 2012.
145. Melo, C.; Dantas, J.; Pereira, P.; Maciel, P. Distributed application provisioning over Ethereum-based private and permissioned blockchain: Availability modeling, capacity, and costs planning. *J. Supercomput.* **2021**, *77*, 9615–9641. [CrossRef]
146. Blackley, J.A.; Peltier, T.R.; Peltier, J. *Information Security Fundamentals*; Auerbach Publications: Boca Raton, FL, USA, 2004.
147. Corbet, S.; Lucey, B.; Urquhart, A.; Yarovaya, L. Cryptocurrencies as a financial asset: A systematic analysis. *Int. Rev. Financ. Anal.* **2019**, *62*, 182–199. [CrossRef]
148. Layouni, F.; Pollet, Y. Fi-orbac: A model of access control for federated identity platform. In Proceedings of the IADIS International Conference Information Systems, Barcelona, Spain, 25–27 February 2009.
149. Rouhani, S.; Deters, R. Blockchain based access control systems: State of the art and challenges. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence, Thessaloniki, Greece, 14–17 October 2019; pp. 423–428.
150. Cherdantseva, Y.; Hilton, J. A reference model of information assurance & security. In Proceedings of the 2013 International Conference on Availability, Reliability and Security, Washington, DC, USA, 2–6 September 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 546–555.
151. Dhillon, G.; Backhouse, J. Technical opinion: Information system security management in the new millennium. *Commun. ACM* **2000**, *43*, 125–128. [CrossRef]
152. Anderson, J.M. Why we need a new definition of information security. *Comput. Secur.* **2003**, *22*, 308–313. [CrossRef]
153. Dhillon, G.; Torkzadeh, G. Value-focused assessment of information system security in organizations. *Inf. Syst. J.* **2006**, *16*, 293–314. [CrossRef]
154. Kolkowska, E.; Hedström, K.; Karlsson, F. Information security goals in a Swedish hospital. In Proceedings of the 8th Annual Security Conference, Las Vegas, NV, USA, 15–16 April 2009; pp. 339–351.
155. Parent Zone. Everything You Need to Know about Cryptocurrency. 2021. Available online: (accessed on 19 August 2022).
156. Skowronski, R. On the applicability of the GRIDNET protocol to Smart Grid Environments. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; Volume 2018, pp. 200–206. [CrossRef]
157. Rehman, S.; Khan, B.; Arif, J.; Ullah, Z.; Aljuhani, A.; Alhindi, A.; Ali, S. Bi-directional mutual energy trade between smart grid and energy districts using renewable energy credits. *Sensors* **2021**, *21*, 88. [CrossRef]
158. Mahmud, H.; Rahman, T. An Application of blockchain to securely acquire, diagnose and share clinical data through smartphone. *Peer-Peer Netw. Appl.* **2021**, *14*, 3758–3777. [CrossRef]
159. Meskini, F.; Islamic, R. Multi-agent based simulation of a smart insurance using Blockchain technology. In Proceedings of the 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), Marrakech, Morocco, 28–30 October 2019. [CrossRef]
160. Wang, Y.; Su, Z.; Zhang, N. Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3620–3631. [CrossRef]
161. Alam Khan, F.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaid, H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain. Cities Soc.* **2020**, *55*. [CrossRef]
162. El Khanboubi, Y.; Hanoune, M. Exploiting Blockchains to improve Data Upload and Storage in the Cloud. *Int. J. Commun. Netw. Inf. Secur.* **2019**, *11*, 1–8. [CrossRef]
163. Peter Wallker, A.; Santhya, R.; Sethumadhavan, M.; Amritha, P. Anonymous Network Based on Software Defined Networking. In Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 15–17 June 2020; pp. 619–624. [CrossRef]
164. Benaddi, H.; Ibrahimi, K.; Dahri, H.; Benslimane, A. A Framework to Secure Cluster-Header Decision in Wireless Sensor Network Using Blockchain. *Commun. Comput. Inf. Sci.* **2020**, *1264*, 205–218. [CrossRef]
165. Mohammad, S.J.; Sial, M.S.; Salman, A.; Omhand, K.; Thu, P.A.; Lewaa, I. Blockchain Technology and the Contemporary Business Models; Connecting Nano Energy Storage Devices with Trade for Investors. *Webology* **2022**, *19*, 2683–2694. [CrossRef]
166. Khalaf, O.; Abdulsahib, G.; Kasmaei, H.; Ogudo, K. A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications. *Int. J. Collab.* **2020**, *16*, 16–32. [CrossRef]
167. Sathya, A.; Banik, B. A comprehensive study of blockchain services: Future of cryptography. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 279–288. [CrossRef]

168. Merkle, R.C. A Digital Signature Based on a Conventional Encryption Function. In *Advances in Cryptology—CRYPTO '87 Proceedings*; Pomerance, C., Ed.; Springer: Heidelberg/Berlin, Germany, 1988; pp. 369–378.
169. Cherckesova, L.V.; Safaryan, O.A.; Lyashenko, N.G.; Korochentsev, D.A. Developing a New Collision-Resistant Hashing Algorithm. *Mathematics* **2022**, *10*, 2769. [CrossRef]
170. IPFS Powers the Distributed Web. Available online: https://ipfs.tech/ (accessed on 19 August 2022).
171. BigChainDB—The Blockchain Database. Available online: https://www.bigchaindb.com/ (accessed on 19 August 2022).
172. Pathak, A.; Patil, T.; Pawar, S.; Raut, P.; Khairnar, S.; Gite, D. Bibliometric survey on Zero-Knowledge Proof for Authentication. *Libr. Philos. Pract.* **2021**, *2021*, 1–26.
173. Li, J. Hash algorithm optimization for long-span digital currency transactions based on multi-constraint optimization. In Proceedings of the 2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS), Chongqing, China, 6–8 December 2019; pp. 560–564. [CrossRef]
174. Shrivastva, N.; Devi, S.; Verma, J. Digital Money: The Empowering New Currency. In Proceedings of the 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2–4 July 2020; pp. 837–840. [CrossRef]
175. Song, H.; Chen, Y. Digital Financial Transaction Security Based on Blockchain Technology. *J. Phys. Conf. Ser.* **2021**, *1744*, 032029. [CrossRef]
176. Suciu, G.; Sachian, M.A.; Vochin, M.; Dobrea, M.; Beceanu, C.; Iosu, R.; Petrache, A. Blockchain applicability using Smart Power Management: SealedGrid Architecture. In Proceedings of the 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), Bucharest, Romania 29 September–2 October 2019. [CrossRef]
177. Moradi, J.; Shahinzadeh, H.; Nafisi, H.; Gharehpetian, G.; Shaneh, M. Blockchain, a Sustainable Solution for Cybersecurity Using Cryptocurrency for Financial Transactions in Smart Grids. In Proceedings of the 2019 24th Electrical Power Distribution Conference (EPDC), Khoramabad, Iran, 19–20 June 2019; pp. 47–53. [CrossRef]
178. He, Y.; Li, H.; Cheng, X.; Liu, Y.; Yang, C.; Sun, L. A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications. *IEEE Access* **2018**, *6*, 27324–27335. [CrossRef]
179. Aldawood, H.; Skinner, G. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet* **2019**, *11*, 73. [CrossRef]
180. Hetler, A. 9 Common Cryptocurrency Scams in 2023. 2022. Available online: https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams (accessed on 19 August 2022).
181. Muchonjo, A.K.; Wanyembi, G.; Makori, C. An Investigation into End Users' Factors Leading to iPredators' Social Engineering Attacks in Cyberspace. *Int. J. Comput. Sci. Inf. Technol. Res.* **2017**, *5*, 180–197.
182. Salahdine, F.; Kaabouch, N. Social engineering attacks: A survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
183. Hare-Brown, N. Confusing terminology stunts the growth of cyber insurance. *Comput. Fraud. Secur.* **2019**, *2019*, 16–17. [CrossRef]
184. Cybersecurity and Infrastructure Security Agency. Security Tip (ST04-014). Avoiding Social Engineering and Phishing Attacks. 2009. Available online: https://seclists.org/cert/2009/38 (accessed on 19 August 2022).
185. Weber, K.; Schütz, A.E.; Fertig, T.; Müller, N.H. Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users. In Proceedings of the International Conference on Human-Computer Interaction, Oldenburg, Germany, 5–8 October 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 650–668.
186. Wei, W. How to Steal Bitcoin Wallet Keys (Cold Storage) from Air-Gapped PCs. 2018. Available online: https://thehackernews.com/2018/04/bitcoin-wallet-keys.html (accessed on 19 August 2022).
187. Weston, S. Coinbase Notifies 6000 Customers of Data Breach. 2021. Available online: https://www.techcentral.ie/coinbase-notifies-6000-customers-of-data-breach/ (accessed on 19 August 2022).
188. Zimdars, M.; McLeod, K. *Fake News: Understanding Media and Misinformation in the Digital Age*; MIT Press: Cambridge, MA, USA, 2020.
189. Conteh, N.Y.; Schmick, P.J. Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*; IGI Global: Hershey, PA, USA, 2021; pp. 19–31.
190. Conteh, N.Y. The dynamics of social engineering and cybercrime in the digital age. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*; IGI Global: Hershey, PA, USA, 2021; pp. 144–149.
191. Goel, D.; Jain, A.K. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Comput. Secur.* **2018**, *73*, 519–544. [CrossRef]
192. Cheng, H.; Regedzai, G.R. A Survey on Botnet Attacks. *Am. Sci. Res. J. Eng. Technol. Sci. (ASRJETS)* **2021**, *77*, 76–89.
193. Chakraborty, M.; Singh, M. Introduction to Network Security Technologies. In *The "Essence" of Network Security: An End-to-End Panorama*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 3–28.
194. Jitendra, N.; Vinay, N.; Ram, P.; Sidhardha, P.N.; Deepthi, D. Text-based shoulder surfing and key logger resistant graphical password. *Eng. Sci.* **2020**, *11*, 214–223.
195. Maigida, A.M.; Olalere, M.; Alhassan, J.K.; Chiroma, H.; Dada, E.G. Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *J. Reliab. Intell. Environ.* **2019**, *5*, 67–89. [CrossRef]
196. Roseline, S.A.; Geetha, S. A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Comput. Electr. Eng.* **2021**, *92*, 107143. [CrossRef]
197. Breda, F.; Barbosa, H.; Morais, T. Social engineering and cyber security. In Proceedings of the International Technology, Education and Development Conference, Valencia, Spain, 6–8 March 2017; Volume 3, pp. 106–108.

198. Ferreira, A.; Coventry, L.; Lenzini, G. Principles of persuasion in social engineering and their use in phishing. In Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust, Berlin, Heidelberg, 2–7 August 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 36–47.
199. Ivaturi, K.; Janczewski, L. A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management. Centre for Information Technology, Organizations, and People, Lisbon, Portugal, 21 May 2011; pp. 1–12.
200. Brody, R.G.; Brizzee, W.B.; Cano, L. Flying under the radar: Social engineering. *Int. J. Account. Inf. Manag.* **2012**, *20*, 335–347. [CrossRef]
201. Heikkinen, S. Social engineering in the world of emerging communication technologies. In Proceedings of the Wireless World Research Forum, Citeseer, 2006; pp. 1–10. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=be5a68ba31989b6d224dd5666a6b2392b067b886 (accessed on 29 May 2022).
202. Workman, M. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Am. Soc. Inf. Sci. Technol.* **2008**, *59*, 662–674. [CrossRef]
203. Tovstukha, I.; Laaneots, U. Prevention Strategies For Social Engineering. 2013. Available online: https://courses.cs.ut.ee/MTAT.03.246/2013_spring/uploads/Main/essay07.pdf (accessed on 19 August 2022).
204. Koyun, A.; Al Janabi, E. Social engineering attacks. *J. Multidiscip. Eng. Sci. Technol. (JMEST)* **2017**, *4*, 7533–7538.
205. Conteh, N.Y.; Staton, Q.N. The Socio-Economic Impact of Identity Theft and Cybercrime: Preventive Measures and Solutions. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*; IGI Global: Hershey, PA, USA, 2021; pp. 104–113.
206. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
207. Kerr, E.; Lee, C.A.L. Trolls maintained: Baiting technological infrastructures of informational justice. *Inf. Commun. Soc.* **2021**, *24*, 1–18. [CrossRef]
208. Mann, I. *Hacking the Human: Social Engineering Techniques and Security Countermeasures*; Routledge: New York, NY, USA, 2017.
209. Berghel, H.; Berleant, D. The Online Trolling Ecosystem. *Computer* **2018**, *51*, 44–51. [CrossRef]
210. Gupta, S.; Singhal, A.; Kapoor, A. A literature survey on social engineering attacks: Phishing attack. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 29–30 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 537–540.
211. Ekawade, S.; Mule, S.; Patkar, U. Phishing attacks and its preventions. *Imp. J. Interdiscip. Res.* **2016**, *2*, 1–4.
212. Alsayed, A.; Bilgrami, A. E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *Int. J. Emerg. Technol. Adv. Eng.* **2017**, *7*, 109–115.
213. Bisson, D. 6 Common Phishing Attacks and How to Protect against Them. Tripwire. 2016. Available online: http://www.tripwire.com/state-of-security/security-awareness/6-commonphishing-attacks-andhow-to-protect-against-them/ (accessed on 5 October 2016).
214. Dadkhah, M.; Jazi, M.D. Secure payment in E-commerce: Deal with Keyloggers and Phishings. *Int. J. Electron. Commun. Comput. Eng.* **2014**, *5*, 656–660.
215. Kontio, M. Social Engineering. Master's Thesis, Turku University, Turku, Finland, 2016; Volume 101.
216. Mishra, S.; Soni, D. Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Gener. Comput. Syst.* **2020**, *108*, 803–815. [CrossRef]
217. Pienta, D.; Thatcher, J.B.; Johnston, A.C. A taxonomy of phishing: Attack types spanning economic, temporal, breadth, and target boundaries. In Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, CA, USA, 13 December 2018; Volume 1, pp. 2216–2224.
218. Badawi, E.; Jourdan, G.V. Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. *IEEE Access* **2020**, *8*, 200021–200037. [CrossRef]
219. Alzahrani, A. Coronavirus social engineering attacks: Issues and recommendations. *IJACSA* **2020**, *11*, 9. [CrossRef]
220. Bhushan, B.; Sahoo, G.; Rai, A.K. Man-in-the-middle attack in wireless and computer networking—A review. In Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA), (Fall), Dehradun, India, 15–16 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
221. Jain, A.K.; Gupta, B. A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterp. Inf. Syst.* **2022**, *16*, 527–565. [CrossRef]
222. Russell, D.L.; Arlow, P.C. *Industrial Security: Managing Security in the 21st Century*; John Wiley & Sons: Hoboken, NJ, USA, 2015.
223. Lan, J.L.; Hu, Y.X.; Zhang, Z.; Jiang, Y.M.; Wang, P.; Wu, J.X. *Future Network Architectures and Core Technologies*; World Scientific: Singapore, 2022.
224. Petrenko, S. *Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation*; CRC Press: Boca Raton, FL, USA, 2022.
225. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97.
226. Ali, R.F.; Dominic, P.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Appl. Sci.* **2021**, *11*, 3383. [CrossRef]

227. Syafitri, W.; Shukur, Z.; Mokhtar, U.A.; Sulaiman, R.; Ibrahim, M.A. Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 39325–39343. [CrossRef]
228. Albladi, S.M.; Weir, G.R. Personality traits and cyber-attack victimisation: Multiple mediation analysis. In *2017 Internet of Things Business Models, Users, and Networks;* IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
229. Yang, P.; Zhao, G.; Zeng, P. Phishing website detection based on multidimensional features driven by deep learning. *IEEE Access* **2019**, *7*, 15196–15209. [CrossRef]
230. Yang, R.; Zheng, K.; Wu, B.; Li, D.; Wang, Z.; Wang, X. Predicting user susceptibility to phishing based on multidimensional features. *Comput. Intell. Neurosci.* **2022**, *2022*, 7058972. [CrossRef]
231. Freed, S.E. Examination of Personality Characteristics among Cybersecurity and Information Technology Professionals. Master's Thesis, University of Tennessee, Chattanooga, TN, USA, 2014.
232. DeWeaver, L.F., III. Exploring How Universities Can Reduce Successful Cyberattacks by Incorporating Zero Trust. Ph.D. Thesis, Colorado Technical University, Colorado Springs, CO, USA, 2021.
233. Leukfeldt, E.R.; Kleemans, E.R.; Stol, W.P. Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *Br. J. Criminol.* **2017**, *57*, 704–722. [CrossRef]
234. Scaife, N.; Carter, H.; Traynor, P.; Butler, K.R. Cryptolock (and drop it): Stopping ransomware attacks on user data. In Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 27–30 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 303–312.
235. Connolly, A.Y.; Borrion, H. Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. *Comput. Secur.* **2022**, *119*, 102760. [CrossRef]
236. Rhoades, A. Big Tech Makes Big Data out of Your Child: The FERPA Loophole EdTech Exploits to Monetize Student Data. *ABLJ* **2020**, *9*, 445.
237. Wen, K. 4 Lessons in-House GCs Can Learn from Law Firm Data Breaches. 2022. Available online: https://www.simplelegal.com/blog/law-firm-data-breaches (accessed on 19 August 2022).
238. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Detecting insider threat via a cyber-security culture framework. *J. Comput. Inf. Syst.* **2022**, *62*, 706–716. [CrossRef]
239. European Parliament. *How to Protect Yourself from Cybercrime*, 2022.
240. Leitão, P.; Queiroz, J.; Sakurada, L. Collective Intelligence in Self-Organized Industrial Cyber-Physical Systems. *Electronics* **2022**, *11*, 3213. [CrossRef]
241. Sultanik, E.; Remie, A.; Manzano, F.; Brunson, T.; Moelius, S.; Kilmer, E.; Myers, M.; Amir, T.; Schriner, S. *Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers*; Technical Report; Trail of Bits: New York, NY, USA 2022.
242. *Software One*; Cybersecurity User Awareness. Protect Your Business Against Social Engineering Threats. 2022. Available online: https://www.softwareone.com/en-ch/solutions/managed-security/cybersecurity-user-awareness (accessed on 19 August 2022).
243. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
244. Fanti, G.; Lipsky, J.; Moehr, O. Central Bankers' New Cybersecurity Challenge. 2022. Available online: https://www.imf.org/en/Publications/fandd/issues/2022/09/Central-bankers-new-cybersecurity-challenge-Fanti-Lipsky-Moehr (accessed on 4 January 2023).
245. Atlantic Council. Central Bank Digital Currency Tracker. 2022. Available online: https://www.atlanticcouncil.org/cbdctracker/ (accessed on 4 January 2023).
246. World Economic Forum. Banking and Capital Markets. 4 Key Cybersecurity Threats to New Central Bank Digital Currencies. 2021. Available online: https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies/ (accessed on 5 January 2023).
247. Salman, A. Digital currencies and the power shift in the economy. *Proceedings of the Creative Business and Social Innovations for a Sustainable Future: Proceedings of the 1st American University in the Emirates International Research Conference—Dubai, UAE 2017*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 123–131.
248. Denecker, O.; d'Estienne, A.; Gompertz, P.M.; Sasia, E. Central Bank Digital Currencies: An Active Role for Commercial Banks. 2022. Available online: https://www.mckinsey.com/industries/financial-services/our-insights/central-bank-digital-currencies-an-active-role-for-commercial-banks (accessed on 6 January 2023).