MITIGATING DIGITAL ASSET RISKS

Huei-Wen Teng, Wolfgang Karl Härdle,
Christian M. Hafner, e.a.

LIDAM Discussion Paper ISBA
2023 / 30

UCLouvain

ISBA | LIDAM
Louvain Institute of Data Analysis and Modeling in economics and statistics

ISBA

Voie du Roman Pays 20 - L1.04.01

B-1348 Louvain-la-Neuve

Email : lidam-library@uclouvain.be

https://uclouvain.be/en/research-institutes/lidam/isba/publication.html

Mitigating Digital Asset Risks

Huei-Wen Teng[1]

Wolfgang Karl Härdle[2]

Joerg Osterrieder[3] Lennart John Baals[4] Vassilios Papavassiliou[5] Karolina Bolesta[6] Audrius Kabašinskas[7] Olivija Filipovska[8] Nikolaos S. Thomaidis[9] Alexios-Ioannis Moukas[10] Sam Goundar[11] Jamal Abdul Nasir[12] Abraham Itzhak Weinberg[13] Veni Arakelian[14] Ciprian-Octavian Truică[15] Mutlu Akar[16] Esra Kabaklarlı[17] Elena-Simona Apostol[18] Maria Iannario[19] Barbara Będowska-Sójka[20] Hanna Kristín Skaftadóttir[21] Catarina Silva[22] Ozgur Yildirim[23] Albulena Shala[24] Suela Vasil[25] Galena Pisoni[26] Coita Ioana[27] Szabolcs Korba[28] Christian M. Hafner[29] Belma Ozturkkal[30] Peter Schwendner[31] Bálint Molnár[32] Elda Xhumari[33] Armela Maxhelaku[34] Daniel Pele[35]

September 17, 2023

[1]Department of Information Management and Finance, National Yang Ming Chiao Tung University, Taiwan. E-mail: venteng@gmail.com.

[2]Blockchain Research Center, Humboldt-Universität zu Berlin, Berlin, Germany; Department of Information Management and Finance, National Yang Ming Chiao Tung University, Hsinchu, Taiwan; Dept Mathematics and Physics, Charles University, Prague, CZ; Sim Kee Boon Institute, Singapore Management U, Singapore, SG; ACI Asia Competitiveness Institute, National University Singapore, Singapore, SG; IDA Insitute of Digital Assets, Academy of Economics Science, Bucharest, Romania. E-mail: haerdle@hu-berlin.de.

[3]Institute of Applied Data Science and Finance, Bern Business School, Brückenstrasse 73, Bern, Switzerland. E-mail: joerg.osterrieder@bfh.ch; The High-Tech Business and Entrepreneurship Group, Faculty of Behavioural, Management and Social Sciences, University of Twente, Enschede, Netherlands. E-mail: joerg.osterrieder@utwente.nl.

[4]Bern University of Applied Science, Bern, Switzerland. E-mail: lennart.baals@bfh.ch.

[5]University College Dublin, UCD Michael Smurfit Graduate Business School and UCD Geary Institute for Public Policy, Carysfort Avenue, Blackrock, Co Dublin, Ireland. E-mail: vassilios.papavassiliou@ucd.ie.

[6]Department of Economics, Warsaw School of Economics, Warsaw, Poland. E-mail: kboles@sgh.waw.pl.

[7]Department of Mathematical modeling, Kaunas University of Technology, Kaunas, Lithuania. E-mail: audkaba@ktu.lt.

[8]Komercijalna Banka AD Skopje, Skopje, North Macedonia. E-mail: olivijaf@gmail.com.

[9]Department of Financial and Management Engineering, University of the Aegean, Chios, Greece. E-mail: nthomaid@fme.aegean.gr.

[10]School of Economics, Aristotle University of Thessaloniki, Thessaloniki, Greece. E-mail: moukalex@econ.auth.gr.

[11]School of Science and Technology, RMIT University, Hanoi, Vietnam. E-mail: sam.goundar@gmail.com.

[12]University of Galway, Ireland. E-mail: jamal.nasir@universityofgalway.ie.

[13]Tel Aviv, Israel. E-mail: aviw2010@gmail.com.

[14]Economic Research and Investment Strategy, Piraeus Bank, Greece & UCL Center for Blockchain Technologies. E-mail: arakelianv@piraeusbank.gr.

[15]University Politehnica of Bucharest, Bucharest, Romania. E-mail: ciprian.truica@upb.ro.

[16]Yildiz Technical University, Istanbul, Turkey. E-mail: makar@yildiz.edu.tr.

[17]Department of Economics, Selçuk University, Konya, Turkey. E-mail: etalasli@selcuk.edu.tr.

[18]University Politehnica of Bucharest, Bucharest, Romania. E-mail: elena.apostol@upb.ro.

[19]University of Naples Federico II, Naples, Italy. E-mail: maria.iannario@unina.it.

[20]Poznań University of Economics and Business, Poznań, Poland. E-mail: barbara.bedowska-sojka@ue.poznan.pl.

[21]University of Iceland, Reykjavík, Iceland. E-mail: hks7@hi.is.

[22]University of Coimbra, Coimbra, Portugal. E-mail: catarina@dei.uc.pt.

[23]Yildiz Technical University, Istanbul, Turkey. E-mail: ozgury@yildiz.edu.tr.

[24]University of Prishtina "Hasan Prishtina" Prishtina, Kosova. E-mail: albulena.shala@uni-pr.edu.

[25]Tirana University, Tirana, Albania. E-mail: suela.maxhelaku@fshn.edu.al.

[26]Universite Cote d'Azur, Biot, France. E-mail: galena.pisoni@univ-cotedazur.fr.

[27]University of Oradea, Oradea, Romania. E-mail: coita.iflorina@gmail.com.

[28]Eötvös Loránd University, Budapest, Hungary. E-mail: korba@inf.elte.hu.

[29]Université catholique de Louvain, Louvain-la-Neuve, Belgium. E-mail: christian.hafner@uclouvain.be.

[30]Department of International Trade and Finance, Kadir Has University, Istanbul, Turkey. E-mail: belma.ozturkkal@khas.edu.tr.

[31]Institute of Wealth & Asset Management, Zurich University of Applied Sciences, Winterthur, Switzerland. E-mail: peter.schwendner@zhaw.ch.

[32]Eötvös Loránd University, Budapest, Hungary. E-mail: molnarba@inf.elte.hu.

[33]Tirana University, Tirana, Albania. E-mail: elda.xhumari@fshn.edu.al.

[34]Tirana University, Tirana, Albania. E-mail: armela.maxhelaku@fdut.edu.al

[35]IDA Insitute of Digital Assets, Academy of Economics Science, Bucharest, Romania. E-mail: danpele@ase.ro

Abstract

The rapid emergence of digital assets, underpinned by technological advancements such as blockchain, distributed ledger technology (DLT), and smart contracts, has triggered a paradigm shift in the global financial ecosystem. These digital assets, which encompass cryptocurrencies, tokenized securities, stablecoins, non-fungible tokens (NFTs), and central bank digital currencies (CBDCs), hold the potential to transform financial markets by enabling new business models, investment opportunities, and efficient transaction mechanisms. However, their accelerated growth also introduces a unique set of challenges and risks, such as fraud, market manipulation, cybersecurity threats, and regulatory uncertainties.

This position paper presents an interdisciplinary, empirical analysis of the digital asset landscape, focusing on the definition and classification of digital assets, their evolution from novelty to necessity, and the current state of adoption and regulation. We explore the various types of digital assets, their unique characteristics and use cases, and the technological innovations that have shaped their development, such as the advent of blockchain technology and the rise of decentralized finance (DeFi) and NFTs. Moreover, we examine the regulatory landscape surrounding digital assets, highlighting jurisdictional approaches, regulatory classifications, and key developments in the space, as well as the challenges and opportunities that regulators face in devising effective regulatory frameworks.

To address the risks associated with the proliferation of digital assets, we outline several mitigation strategies and recommendations for regulators, market participants, and stakeholders based on quantitative analysis and empirical findings. These include balancing innovation and risk, by formulating regulations that safeguard the interests of consumers and investors while fostering an environment conducive to innovation; promoting global regulatory coordination and harmonization, to reduce the potential for regulatory arbitrage and enhance cross-border cooperation; and leveraging regulatory sandboxes and innovation hubs, to support the growth of digital asset businesses and facilitate continuous learning and adaptation.

By adopting a forward-looking and flexible approach to regulation and engaging in ongoing dialogue with market participants and stakeholders, regulators can ensure that the benefits of digital assets are realized while mitigating the associated risks.

Keywords: Digital assets; Blockchain technology; Regulatory frameworks; Decentralized finance (DeFi); Non-fungible tokens (NFTs)

JEL Codes: G2; E4; K2; L5; O3; O1

Contents

List of Tables

List of Figures

1 Digital assets

The exponential proliferation of Digital Assets (DAs) in the global financial ecosystem has garnered significant attention from scholars, regulators, and market participants. These novel financial instruments pose unique opportunities and challenges, necessitating a comprehensive understanding of their implications for financial stability and regulatory oversight. Limited interconnections with the traditional financial system and no significant financial services outside the ecosystem make the DA ecosystem intransparent and possibly fragile. As a starting point, this section outlines the definitions and classifications of DAs, laying the foundation for subsequent in-depth analysis.

In summary, the evolution of DAs from novelty to necessity has been characterized by technological advancements, diversification, integration into the traditional financial system, and increasing institutional adoption. This trajectory underscores the importance of understanding and addressing the risks associated with their proliferation in order to maintain a stable and resilient global financial ecosystem.

1.1 Definition and Classification of DAs

DAs, in the context of contemporary financial systems and technology, can be comprehensively defined as electronic data or content that possesses inherent, transactional, or functional value. The digital representation of this value, which is cryptographically recorded on a secured distributed ledger or any similar technology is the DA. The emergence and proliferation of these assets are attributable to the ongoing digital transformation of the global economy, which has consequently given rise to novel business models, investment prospects, and risk factors.

These assets, which encompass a broad range of digital entities, exhibit diverse attributes and can be manifested in a multitude of formats. Furthermore, DAs are created, preserved, administered, and transacted via digital channels and technological infrastructures. The blockchain provides the foundation of the digital ecosystem, it is a distributed ledger system having decentralised applications recording transactions between participants. Given their inherent complexity and rapidly evolving nature, DAs warrant meticulous examination and scrutiny in order to better comprehend their underlying characteristics and implications for both traditional and emerging financial ecosystems. Consequently, this understanding facilitates the development of strategies and frameworks aimed at mitigating potential risks and leveraging the opportunities presented by DA innovation within the financial sector.

Different regulators offer different definitions of classifications. To provide a comprehensive understanding of DAs and their associated risks, it is crucial to classify them based on their characteristics, functionalities, and use cases. We took here the liberty to concentrate on the most liquid DAs. The following classification categories can be utilized to categorize DAs.

1. CCs: CCs are decentralized digital currencies that use cryptography for secure transactions and control of new unit creation. Examples of CCs include Bitcoin, Ethereum, and Litecoin. They are primarily used as a medium of exchange, store of value, and unit of account.

2. Utility Tokens: Utility tokens are DAs that represent access to a specific product or service within a platform or ecosystem. These tokens can be used for various purposes, such as purchasing goods and services, voting on platform decisions, or accessing exclusive content. Examples include Basic Attention Token (BAT) and Filecoin (FIL).

3. Security Tokens: Security tokens are digital representations of traditional securities, such as stocks, bonds, or real estate. They are subject to securities regulations and offer rights to ownership, dividends, profit sharing, or interest payments. Examples of security tokens include tokenized stocks and real estate investment tokens.

4. Non-Fungible Tokens (NFTs): NFTs are unique DAs that represent ownership of a specific item or piece of content, such as digital art, collectibles, or virtual real estate. Each NFT has a distinct value recorded in a blockchain and cannot be exchanged on a one-to-one basis with another NFT. Examples include CryptoKitties and NBA Top Shot collectibles.

5. Central Bank Digital Currencies (CBDCs): CBDCs are digital forms of sovereign currencies issued by a country's central bank. CBDCs can be used as a medium of exchange, store of value, and unit of account, similar to traditional currencies. Examples include the Digital Yuan and the proposed Digital Euro.

6. Stablecoins: Stablecoins are DAs that are designed to maintain a stable value by being pegged to a reserve of assets, such as fiat currency, commodities, financial instrument, or other CCs. Examples include Tether (USDT), USD Coin (USDC), and DAI.

The classification of DAs is not mutually exclusive, as some assets can exhibit characteristics of multiple categories. It is crucial to understand the interactions and interdependencies between different types of DAs, as they can influence the risks associated with their increased use. For instance, decentralized finance (DeFi) platforms often rely on a combination of CCs, utility tokens, and stablecoins to facilitate lending, borrowing, and trading services. A proper analysis of such interdepencies requires a dynamic network view on varying nodes and interconnectiveness. An early example of such a network view on CCs can be found in Guo et al. (2022)  https://quantinar.com/course/50/cryptonetworks.

1.2 Evolution of DAs

The emergence of DAs can be traced back to the early days of electronic money and digital cash systems. In comparison to credit card transactions, blockchain-based technology still lags in speed; however, its adoption is rapidly gaining momentum and promises potential advancements in the near future. These precursors to modern DAs laid the groundwork for the evolution of the DA ecosystem that we witness today.

1. The Emergence of Digital Currencies: Prior to the advent of blockchain-based CCs, there were several attempts to create digital currencies using centralized systems. David Chaum, a pioneer in cryptography and privacy, proposed the concept of eCash in the 1980s, see e.g. Judmayer et al. (2017). This digital cash system utilized

blind signatures, allowing users to make anonymous transactions. In the 1990s, DigiCash, an electronic money corporation, was founded by Chaum to implement his eCash concept. However, due to various challenges, including limited adoption, DigiCash ultimately filed for bankruptcy in 1998.

2. Early DA Ecosystems: Following DigiCash, other digital currency initiatives emerged, such as e-gold and Liberty Reserve. E-gold, launched in 1996, was a centralized digital currency platform where users could store and transact digital gold. However, e-gold was plagued by legal issues related to money laundering, leading to its eventual shutdown in 2009. Similarly, Liberty Reserve, founded in 2006, facilitated digital currency transactions using its own digital currency, the Liberty Reserve Dollar (LRD). Liberty Reserve encountered similar issues as e-gold, with its operations ceasing in 2013 due to allegations of money laundering.

As illustrated in Table 1, the evolution of DAs encompasses several stages, each contributing to the transformation of DAs from a novelty to a necessity within the modern financial landscape.

Table 1: Evolution of DAs: From Novelty to Necessity

Stage	**Description**
Historical Context and Early DAs	The Emergence of digital currencies and early DA ecosystems.
Blockchain Technology and CCs	The advent of blockchain technology, Bitcoin, and the expansion of the CC landscape.
Developments in Tokenization	The rise of Initial Coin Offerings (ICOs), token sales, and the tokenization of real-world assets.
DeFi	The growth of DeFi platforms, services, and ecosystems.
NFTs	The emergence of NFTs, digital collectibles, and their applications in various industries.
CBDCs	Motivations, objectives, and developments in CBDC projects worldwide.
Challenges and Risks	Security, infrastructure, regulatory, compliance, and environmental considerations in the evolution of DAs.

These early DA ecosystems faced limitations, such as centralized control, regulatory challenges, and security vulnerabilities (Härdle et al., 2020). The advent of blockchain technology and the introduction of Bitcoin, a decentralized CC, addressed several of these limitations and marked a significant milestone in the evolution of DAs.

1.3 The Advent of Blockchain Technology and CCs

The emergence of blockchain technology and CCs marked a transformative period in the evolution of DAs. Decentralization, security, and trustless transactions were some of the key characteristics that set these novel assets apart from their predecessors.

1. Bitcoin, A Pioneering CC: In 2008, an individual or group of individuals under the pseudonym Satoshi Nakamoto published the Bitcoin whitepaper, which detailed the first implementation of a decentralized, peer-to-peer

Figure 1: An adaptive CC index, Royalton Partners https://www.royalton-partners.com/royalton_crix_crypto_index/

electronic cash system. Bitcoin's underlying technology, the blockchain, is a distributed ledger maintained by a network of nodes, which utilize cryptographic techniques to secure transactions and achieve consensus without a central authority. Bitcoin introduced the proof-of-work (PoW) consensus mechanism, which relies on miners to solve complex mathematical problems, verify transactions, and add new blocks to the blockchain. This decentralized system eliminated the need for intermediaries, such as banks or payment processors, and addressed many of the challenges faced by earlier digital currency initiatives.

2. The Expansion of CC Landscape: Following the success of Bitcoin, numerous alternative CCs, or altcoins, began to emerge. Some of these altcoins aimed to improve upon Bitcoin's design or focus on specific use cases. For example, Ethereum, launched in 2015, introduced a Turing-complete programming language and smart contract functionality, allowing developers to create decentralized applications (dApps) and automate transactions. Litecoin, another notable altcoin, was designed to provide faster transaction processing times compared to Bitcoin. The advent of these CCs spurred innovation in the DA space, leading to a diverse and expansive ecosystem with various blockchain platforms, token standards, and consensus mechanisms.

The advent of blockchain technology and the subsequent proliferation of CCs have given rise to a multitude of use cases and applications, driving the ongoing evolution of DAs and transforming the landscape of financial systems and services. The earliest attempt to create a CC Index is - to the best of our knowledge - the CRIX project. See Trimborn and Härdle (2018), Figure 1, and Royalton CRIX listed in S&P Global. A general introduction into CCs is available in the courselet https://quantinar.com/course/22/crypto.

1.4 NFTs and Digital Collectibles

NFTs represent a unique class of DAs that exhibit distinct characteristics, unlike CCs, which are fungible and interchangeable. NFTs are based on blockchain technology, primarily the Ethereum network, and leverage token standards, such as ERC-721 and ERC-1155, to create provably scarce, indivisible, and non-interchangeable digital tokens. NFTs have gained significant traction in recent years, particularly in the realm of digital art, collectibles, and virtual goods.

NFTs emerged as a novel way to tokenize unique DAs, with the primary innovation being the ability to create digital scarcity and establish true ownership. NFTs can represent a wide range of digital and physical assets, such as art, virtual real estate, in-game items, domain names, and intellectual property.

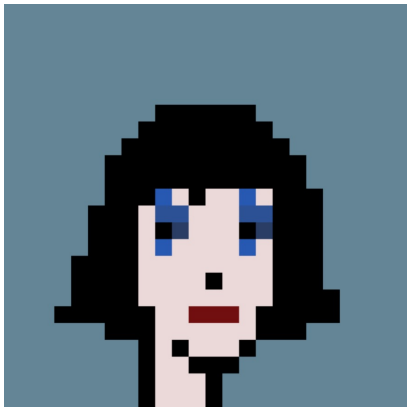

Figure 2: A cryptopunk from larvalabs.com

The market for NFTs has experienced exponential growth in recent years, driven by various applications and use cases: NFTs have disrupted the digital art and collectibles markets, enabling artists to tokenize their creations and sell them through NFTs marketplaces. NFTs provide artists with new revenue streams, as they can earn royalties on secondary market sales. NFTs play a crucial role in virtual worlds and metaverse platforms, such as Decentraland https://decentraland.org and The Sandbox https://www.sandbox.game/en/nft/, where users can buy, sell, and trade virtual land, buildings, and other DAs as NFTs. NFTs enable the tokenization of in-game items, such as skins, weapons, and characters, facilitating true ownership and the ability to trade these items across different games and platforms. NFTs have potential applications in intellectual property management and licensing, enabling creators to tokenize and sell licenses for their creations, such as music, software, or patents.

The rapid growth of NFTs has had a profound impact on various industries, particularly in the realm of digital art and virtual goods. As the technology and market for NFTs continue to evolve, new use cases and applications are expected to emerge, further driving the adoption of non-fungible tokens and reshaping the landscape of DAs. A prominent example of NFT business chances is given by the numerous digital art pieces of larvalabs.com, of which a subclass of NFTs is indexing the cryptopunk, see Figure 2.

NFTs are becoming a nascent phenomenon as we ride the wave of digital transformation. In March 2021, an NFT (a single piece of digital art) created by Mike Winklemann a.k.a. Beeple sold for a whopping USD 69.3 million. According to Businesswire.com (June 2023), the global NFTs Market size was valued at USD 16 billion in 2021 and is poised to grow from USD 21.39 billion in 2022 to USD 212 billion by 2030, growing at a CAGR of 33.7% in the forecast period (2023-2030). NFTs come in different forms, represent different rights, and can be an important asset class for investors. DAs, NFTs, and CCs are volatile with the market often crashing and investors losing money, and speculation (value moving up and down).

NFTs and DAs (tokens) are mostly unregulated, and many central banks have taken a "hands-off" approach. On one hand, while investments in these tokens are growing, on the other hand, the market has been volatile (Yousaf and Yarovaya, 2022) thus posing high risks amidst high returns. Investors, financial markets, and policy makers are looking for guidelines and frameworks (Urom et al., 2022) to invest sustainably with minimum risks and maximum returns. Researchers like Wilson et al. (2022) looked at NFTs and how they are used by various

industries, and the opportunities and risks they present. Moreover, Trevisi et al. (2022), provide business models, legal aspects, and market valuation of NFTs, and argue that all NFTs are not created equal and hence are sold with different rights. Therefore, the legal aspects and market valuation need careful scrutiny so that business models may be built appropriately.

NFTs are hot and trending amongst crypto investors. There are a few who understand the mechanics of NFTs and are working on this technology. The market for NFTs is characterized as high-risk, high return, generally shrouded in secrecy, and a market with low participation relative to conventional investment markets.

Investors must exercise caution and conduct thorough due diligence before entering the NFT market. Additionally, the authenticity and provenance of NFTs play a significant role in determining their economic value. Counterfeit or unauthorized NFTs can undermine market trust and diminish the overall value of genuine NFTs. The emergence of fraudulent activities and copyright infringements in the NFT space necessitates the development of robust mechanisms for verification and validation. Strengthening security measures, implementing blockchain-based solutions, and promoting transparent ownership records can mitigate risks and enhance the value proposition of NFTs (Flick, 2022). A recent synthesis paper from IMF (IMF and FSB, 2023), summarizes the main risks of DA's from the point of view of macroeconomic stability and concludes that widespread adoption of DA's could disrupt monetary policy and fiscal stability. Emerging Markets and Developing Economies face heightened risks due to stronger incentives for crypto-asset use and limited regulatory capacities.

1.5 CBDCs and the Future of Money

CBDCs represent a new form of digital money that is issued and backed by central banks. CBDCs aim to modernize the existing monetary system by leveraging digital technologies, such as distributed ledgers and cryptography, to enable more efficient, secure, and accessible payment systems. CBDCs have gained significant attention from central banks and policymakers worldwide as they explore the potential benefits and challenges of implementing digital currencies in their respective jurisdictions.

Designing a CBDC requires addressing several technical and economic considerations, such as:

- Architecture: CBDCs can be designed using a centralized, decentralized, or hybrid architecture, depending on the desired degree of control and involvement by the central bank and other intermediaries.
- Access: CBDCs can be designed for retail (general public) or wholesale (financial institutions) use, with varying degrees of accessibility and transactional capabilities.
- Privacy: Balancing privacy and regulatory compliance is a key challenge in CBDC design, as central banks must strike a balance between user privacy and the need for transparency to prevent illicit activities such as money laundering and terrorist financing.
- Interoperability: CBDCs must be designed to be interoperable with existing payment systems and other digital currencies, enabling seamless cross-border transactions and currency exchanges.

Some countries, such as China and the Bahamas, having already launched their digital currencies. These pilot projects and developments can be broadly categorized into two types:

- Retail CBDCs: Aimed at the general public, retail CBDCs facilitate digital payments and transactions between consumers, businesses, and financial institutions. The Bahamian Sand Dollar and the Chinese Digital Currency Electronic Payment (DCEP) are examples of retail CBDCs currently in circulation.
- Wholesale CBDCs: Intended for use by financial institutions, wholesale CBDCs facilitate interbank transactions and settlements, enabling more efficient and secure financial operations. Projects like Project Ubin in Singapore https://www.mas.gov.sg/schemes-and-initiatives/project-ubin, and Project Stella in the European Union and Japan https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf focus on exploring the potential benefits of wholesale CBDCs.

As the development and adoption of CBDCs continue, their potential to transform the global monetary system and reshape the future of money becomes more apparent. It is crucial for central banks and policymakers to address the technical, regulatory, and economic challenges associated with CBDCs to ensure a successful transition to a digital monetary system.

CBDC's access and circulation are confined to designated agents under certain regulatory and policy constraints, similar to central bank reserves today. Typically, these agents are banks and other select financial institutions. In theory, wholesale CBDC is a variant of the current reserve accounts kept at the central bank and electronically mobilized.

A CBDC that can be used by a larger number of agents. In theory, it means all agents within a specific jurisdiction and beyond. In the latter scenario, nonresident people and entities would have access to CBDC (World Bank, 2021).

CBDC could be viewed as a third form of base money, in addition to (i) overnight deposits with the central bank, which are currently only accessible to banks, specific non-bank financial firms, and some depositors in the official sector; and (ii) banknotes, which are widely available but arguably inefficient and dependent on antiquated technology.

According to Bindseil (2019), two alternative technical formats could be used to carry out the CBDC's general purpose: (1) All households and corporations could be granted CBDC by deposit accounts with the central bank. This is not particularly revolutionary in terms of technology; instead, it involves reducing the number of bank accounts that are already available. Commercial banks would offer this service and charge a competitive fee (akin to current ATM fees) to exchange bank deposits for CBDC and banknotes. (2) The central bank could provide a digital token currency that would function without a central ledger and in a decentralized manner. This is frequently connected to anonymity, which implies that the central bank would not know who now possesses the issued tokens (as in the case of banknotes). According to the World Bank (2021), the following important design features should be considered in CBDC: i. anonymity; ii. availability; iii. interest; iv. transfer mechanism: peer-

to-peer (P2P) versus via an intermediary; v. limits or caps (for more information, see the World Bank Document, 2021).

Fernández-Villaverde et al. (2020, 2021) study the implications of bank runs. They demonstrate how implementing CBDC eliminates the risk of a bank runs by encouraging a flow of deposits from the banking system toward the central bank. Keister and Monnet (2020) also consider CBDC's potential effects on bank runs while concentrating on the effectiveness of government interventions. According to its structure, CBDC enables the central bank to more precisely assess the state of the banking industry and swiftly act to reduce the run risk. Keister and Monnet (2020) also consider CBDC's potential effects on bank runs while concentrating on the effectiveness of government interventions. According to its structure, CBDC enables the central bank to more precisely assess the state of the banking industry and swiftly act to reduce the run risk.

Central banks will face several difficulties in implementing CBDC. These are political, economic, technical, and legal difficulties that all need to be resolved. Determining whether central banks give households direct access to their balance sheets will be crucial. Indeed, pressure from the direct involvement of central banks via CBDC may result in future reductions if the unit costs of financial services have remained the same over time. This solution is now very doubtful because of the technical and political economy-related obstacles that must be solved. Even if the adoption of CBDC does not compromise the ability to manage inflation, digital money equivalents cannot address all causes of financial instability. Events in the real world could result in very different results. CBDC will likely impact the relative holdings of important currencies. One reason to exercise caution is that using CBDC as a tool to facilitate cross-border payments and to promote the creation of a larger portfolio of assets denominated in different currencies can result in enormous coordination issues (again, of a technical and political-economic nature). Additionally, the additional duties placed on central banks may not be welcomed if CBDC blurs the distinction between fiscal and monetary policies (Chen and Siklos, 2022).

From the standpoint of payments, a country's choice to implement CBDC should begin with determining its possible advantages compared to current systems and instruments and carrying out a comprehensive analysis of anticipated costs and benefits as well as market structures. Efficiency, encouraging innovation, and enhancing the central bank's function might be used as broad categories to describe the possible advantages of CBDC. However, there are alternative ways to obtain these advantages. The significance, relative weight, and relative benefits of CBDC over alternative options would all depend on the particulars of each country's situation.

The fact that CBDC provides a means of overcoming the zero lower bound of interest rates is another aspect of banks. Furthermore, commercial banks will likely argue that the inclusion of deposit-like features in CBDC will interfere with their ability to act as intermediaries, even though, as was already mentioned, the threat of disintermediation also looms large due to non-financial firms' capacity to replicate traditional commercial bank deposits essentially. Central bank independence may be threatened by the potential blending of monetary and fiscal policies. The expenses incurred in the "production" of CBDC would not be those incurred in the handling, printing, storing, and shipping physical cash. As a result, the cost of issuing CBDCs would be cheaper than the cost

of issuing cash, increasing seigniorage (all other things being equal). However, the central bank might be required to run payment systems that accommodate CBDCs, depending on the CBDC's design. It would be necessary to analyze the overall impact of the abovementioned savings and their costs. In addition to their traditional duty of producing money, central banks now frequently act as the operators of retail payment systems, interacting directly with both market participants and, in some instances, end users. This puts them in a unique position to take on CBDC projects with global reach, which demand leadership, collaboration, and involvement with numerous stakeholders that no other economic player could match. In minimal and fragile states, where printing banknotes would be expensive or would require replacing due to widespread fraud, CBDC might even give central banks a chance to print money (World Bank, 2021).

BIS supports central banks for monetary and financial stability and BIS Innovation HUB has a target to use DeFi to provide open protocol for improvement on speed, and reduction of cost and increasing transparency by providing technological solutions to central banks for advanced functioning of the financial system.

1.6 Developments in Tokenization

Tokenization refers to the process of converting real-world assets, rights, or utilities into digital tokens on a blockchain platform. These tokens can represent a wide range of tangible and intangible assets, enabling more efficient, secure, and transparent management, trading, and transfer of value.

1. Initial Coin Offerings (ICOs) and Token Sales: The emergence of Initial Coin Offerings (ICOs) marked a significant development in the tokenization landscape. ICOs are fundraising mechanisms where projects issue digital tokens, typically on platforms like Ethereum, in exchange for CCs such as Bitcoin or Ether. These tokens can represent various forms of value, such as equity, utility, or access rights. ICOs gained popularity in the mid-2010s as an alternative to traditional venture capital financing, enabling startups and projects to raise funds quickly and with minimal regulatory oversight. However, the lack of regulation and widespread fraud in the ICO space led to increased scrutiny from regulatory bodies, resulting in the decline of ICOs and the emergence of alternative fundraising methods, such as Security Token Offerings (STOs) and Initial Exchange Offerings (IEOs).

2. Tokenization of Real-world Assets: The tokenization of real-world assets, such as real estate, art, and commodities, represents another significant development in the DA space. Tokenization allows for the fractional ownership of high-value assets, providing increased liquidity, lower barriers to entry, and more efficient marketplaces. By leveraging blockchain technology, tokenized assets can be traded and transferred securely and transparently, enabling the creation of new investment opportunities and financial products. Furthermore, tokenization can also facilitate more efficient asset management and tracking by streamlining processes like settlement, clearing, and auditing. As the technology and regulatory environment continue to evolve, the tokenization of real-world assets is expected to gain further traction and transform traditional asset markets.

Developments in tokenization have expanded the scope and potential of DAs, enabling a more inclusive and efficient financial system. The ongoing advancements in this domain are poised to further revolutionize the management, exchange, and ownership of various forms of value.

1.7 The Rise of DeFi

DeFi is a rapidly growing segment of the DA ecosystem that leverages blockchain technology, smart contracts, and decentralized protocols to create financial services and applications without relying on traditional financial intermediaries. DeFi aims to create a more open, transparent, and accessible financial system, and has seen significant advancements in recent years.

1. DeFi Platforms and Services: DeFi platforms are built on top of blockchain networks, primarily Ethereum, which enables the development and deployment of smart contracts. These smart contracts are self-executing programs that encode the rules and logic of financial transactions, allowing for the creation of various DeFi services, such as lending, borrowing, trading, and asset management. Key DeFi services include:

- Decentralized Exchanges (DEXs): DEXs facilitate peer-to-peer trading of DAs without relying on a centralized order book or intermediary. They employ automated market makers (AMMs) and liquidity pools to enable decentralized, trustless trading.
- Lending and Borrowing Platforms: These platforms enable users to lend and borrow DAs through smart contracts, often using over-collateralization to mitigate risks. Interest rates are determined algorithmically based on supply and demand dynamics. A prominent example is aave.com. See  https://quantinar.com/course/174/On-Crypto-backed-Loans.
- Yield Farming and Liquidity Mining: Users can deposit DAs into DeFi protocols to provide liquidity and earn rewards in the form of native platform tokens, often resulting in high annual percentage yields (APYs).
- Derivatives and Synthetic Assets: DeFi platforms offer derivatives and synthetic assets that track the price of underlying assets, such as stocks or commodities, enabling users to gain exposure to a variety of asset classes without direct ownership.

2. The Growth of DeFi Ecosystem: The DeFi ecosystem has experienced exponential growth in recent years, with billions of dollars locked in various DeFi protocols. This growth can be attributed to several factors, including the rise of stablecoins, increased demand for decentralized financial services, and innovations in DeFi infrastructure, such as layer 2 scaling solutions and cross-chain bridges. However, the rapid expansion of DeFi has also introduced new risks and challenges, including smart contract vulnerabilities, high gas fees, and regulatory uncertainty.

The ongoing development and adoption of DeFi have significant implications for the broader financial ecosystem, potentially disrupting traditional financial services and introducing new opportunities for innovation, efficiency,

and financial inclusion. As DeFi continues to evolve, it is crucial to address the technical and regulatory challenges that may hinder its potential to reshape the financial landscape. DeFi, while employing distinct methods, closely aligns with traditional finance in its core functions. By mirroring these aspects, DeFi could potentially magnify inherent vulnerabilities of the financial system (IMF and FSB, 2023).

1.8 Challenges and Risks

As DAs continue to evolve and gain mainstream adoption, they present various challenges and risks that must be addressed by stakeholders, including regulators, developers, and users. Some of these challenges and risks include:

1. Technical Challenges: DAs face several technical challenges, such as:

   - Scalability: Many blockchain networks, including Ethereum and Bitcoin, struggle with scalability issues, resulting in slow transaction processing times and high fees. Layer 2 solutions and alternative consensus mechanisms, such as proof-of-stake (PoS), are being explored to address these challenges.
   - Interoperability: The lack of interoperability between different blockchain platforms and DA ecosystems hinders seamless transactions and asset transfers. Cross-chain technologies, such as bridges and atomic swaps, are being developed to facilitate more efficient and seamless transactions between networks.
   - Security: The security of DAs and blockchain platforms is paramount, as vulnerabilities in smart contracts or consensus mechanisms can lead to significant financial losses. Ongoing research into formal verification, secure programming languages, and cryptographic techniques aims to improve the security and robustness of DA ecosystems.

2. Regulatory and Legal Challenges: The rapid growth and innovation in DAs have outpaced existing regulatory frameworks, leading to several regulatory and legal challenges, such as:

   - Regulatory Uncertainty: The lack of clear regulatory guidelines and classifications for DAs creates uncertainty for developers, investors, and users, potentially hindering innovation and market growth.
   - Anti-Money Laundry (AML)/Know Your Customer (KYC) Compliance: AML and KYC regulations present challenges for DA platforms, as they must balance user privacy with the need for transparency to prevent illicit activities.
   - Taxation and Reporting: The complexities of DA taxation and reporting requirements can create challenges for individuals and businesses, necessitating the development of more streamlined and user-friendly tools and guidelines.

3. Market Risks: The DA market is characterized by volatility and rapid fluctuations, exposing investors and users to various market risks, such as:

- Price Volatility: The high price volatility of DAs can lead to significant financial losses for investors and users, particularly in the case of leveraged trading or margin calls.
- Liquidity Risk: The liquidity of DA markets can vary significantly, with some assets experiencing low trading volumes or wide bid-ask spreads, making it challenging for users to buy or sell assets at desired prices.
- Market Manipulation: The DA market is susceptible to manipulation, such as pump-and-dump schemes or wash trading, which can create artificial price movements and mislead investors.

2 Multifaceted Risk Structures

2.1 Technological Risks

With an increased degree of complexity in the contract mechanisms of DAs, investors tend to face higher risks that are specifically linked to the (opaque) character of the digital instruments. For DeFi assets with fully automated transactions, Azar et al. (2022) and Zihan et al. (2023) identify limits for investors to thoroughly assess the risk characteristics of the DAs.

Centrally to the point of mitigating technical/technological risks is the reduction of smart contract complexity. Currently, the existing degree of complexity underlying smart contracts (distributed networks & asymmetric cryptography amongst others) makes it difficult to evaluate many claims concerning their actual capabilities and risk characteristics Mik (2017). Emphasizing or establishing trust in the technological architecture of DAs enhanced by smart contracts is vital to ensure investors that the instruments function reliably. Mistakes or bugs inherent to in-transparent contract code will inversely cause financial harm and lead to significant losses for investors. Hence, a lack of transparency in the technical design and functioning of DeFi-related DAs may thus stand out as a severe technological risk factor. Nevertheless, transparency risk might not always originate from the individual asset itself but can also rather be associated with the overarching decentralized exchange (DEXs) that may not disclose the underlying algorithms for price determination or the actual list of tokens traded on the platform. This opacity might also make it difficult for investors to assess risks that are linked to a particular asset.

Furthermore, in close analogy with the risk of contract complexity, individual unfamiliarity with the technological facets of blockchain transactions itself remains another factor that substantially contributes to user-induced technology risk for DA investors. Adequate risk assessment of many DAs requires a substantial understanding of the blockchain and underlying protocols that characterize the respectively distributed ledger. For retail investors with little or insufficient knowledge about these features, a proper assessment of the technological risk factors may thus be infeasible.

While blockchain technologies are inherently designed to be secure and resilient, they are not without their vulnerabilities. Blockchain networks, for instance, are susceptible to Sybil attacks, where an attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, and uses them to gain a disproportionately large influence Douceur (2002). In this context, blockchain networks can also be

vulnerable to routing attacks. This case would relate to an attacker taking control of the Internet Service Provider (ISP) and manipulating the routes to partition the network or delaying the block propagation, ultimately leading to double-spending Apostolaki et al. (2017). Therefore, technological risk factors in relation to the DLT technology underlying certain DAs should also concern investors in their overall risk assessment.

Moreover, with the rapid expansion of the DeFi space and the introduction of DEXs, many DAs became more interconnected with other crypto assets and blockchain networks. The Ethereum blockchain is the leading platform for smart contracting Kaal (2020) and conversely the technological and financial stability of its CC Ether (ETH) has hence implications for DeFi markets. NFTs are subject to specific risks associated with the related smart contracts. If, for example, the NFT represents a digital art object (see Figure 2), the ownership of the object is identified on the blockchain, but the object itself might be stored elsewhere, e.g. on a website. The blockchain is immutable, but the website is not, hence there is a risk that the DA, to which a pointer on a blockchain refers to, no longer exists.

The risks of CCs stem from two main issues: their platform (usually blockchain-based) and their usage. Roohparvar (2022) list the relevant risks (Kubicek, 2018; Șcheau et al., 2020):

Crypto-malware and Ransomware: Cryptomalware is malware that uses non-authorized computational resources to mine CCs. Ransomware is a type of malware that threatens to publish the victim's personal data or block or sell the CC that is stored in victim's account. Malware is typically injected as malicious code from websites, advertisements, or infected trading platforms Connolly and Wall (2019). There are several solutions in the market known as anti-malware solutions. Usually, they restrict access to common ransomware at entry points. They used proxy servers for internet access and ad-blocking software.

Using Third-Party Software: Usually, CC investors use third-party tools for different tasks and purposes. Regulations and a whitelist of such tools can be a countermeasure for this risk.

Illegal Trading Platforms: CC trading platforms are not mature, and hence their trustworthiness level is not always known. In addition, to the best of our knowledge, there are no regulations that promise that the web trading platform can meet the required levels of trustworthiness. As a result, there is potential for multi-level marketing scams, hacking, or data leaks. Countermeasures can be regulations and security tests that promise the required trustworthiness level.

Phishing Attacks: An attacker steals the CC holder's private keys or personal information. This is achieved through the impersonation of an eligible source. From that moment, the victim responds to the attacker and the attacker typically masquerades as a legitimate entity Roohparvar (2022). One popular way to countermeasure this attack is to use a secure email gateway that recognizes the email source and reliability level. In this way, it blocks emails with a harmful potential.

Security of CC Accounts: The access to CC account is based on a password that creates a private key behind the scenes. If a password is hacked or stolen, it is not possible to recover it. One of the countermeasures is to use password Multi-Factor authentication (MFA) to ensure that the password holder is the right person.

CC Exchanges that are not Regulated: One characteristic of CC is decentrality. This is usually a by-product of the blockchain architecture. Practically, decentralized architecture does not allow anybody to control or regulate it. One of the proposed approaches is the establishment of a governing body, such as the Central Bank Digital Currency (CBDC), which will be in charge of the production, management, and regulation of CC.

User Perplexity: CC is based on new technologies and uses different jargons and concepts. As a result, investors find this difficult to comprehend. CCs are considered risky by investors. One way to cope with this is to make the technology more accessible and user-friendly to users. This can also be achieved by establishing helpdesks for users.

Web application firewall filters and monitors the HTTP traffic that moves between a web application and the Internet in order to assist in the protection of web applications. WAFs are designed to protect web applications against attacks such as cross-site forgery, cross-site scripting (also known as XSS), file inclusion, and SQL injection, amongst others.

MFA adds an additional layer of security to DAs by requiring users to provide multiple forms of authentication, such as a password and a biometric factor or a code sent to their phone. Digital wallets are designed to store DAs securely using encryption and other security measures, in order to reduce the risk of unauthorized access and theft of DAs.

Recent literature also stressed the importance of data privacy and systems for banking and financial services. When financial data and applications can be accessed from remote locations, there may be potential risks of data leakages, and respectively privacy invasions, and identity thefts, associated often with risks of loss of money. A constant evaluation of security frameworks used by banks and financial institutions is needed to cope with new mechanisms for data breaches. Faced with these different threats, security continues to be a priority for banking and financial institutions.

DORA is an existing regulation from the EU regarding technological, security, and infrastructural risks in the finance domain; It sets unique requirements regarding the security of network and information systems of companies and organizations operating in the financial sector and the critical third parties that provide information and communication technology (ICT)-related services to them, such as cloud platforms or data analytics services. With it, financial companies are obliged to respond to and recover from all types of ICT-related disruptions and threats, thus reducing the possibility of security and infrastructural damages.

Significant issues still need to be addressed to mitigate risks in relation to infrastructure risk and management in relation to crypto-assets as well. One issue is the availability of adequately trained staff to perform relevant infrastructure risk detection and fixes, therefore readiness to implement these techniques is in general low in companies. Now, after the introduction of MiCA regulation, this becomes of big importance for crypto companies. The provided deadline of July 2024 to adapt may be too stringent for some.

2.2 Legal and Regulatory Risks

The current state of DAs adoption and regulation encompasses a rapidly evolving landscape, with various stakeholders and regulatory bodies adapting to the unique challenges and opportunities presented by these innovative financial instruments. This subsection delves into the technical aspects of DAs adoption, while examining the complex regulatory landscape, as both aspects play a critical role in shaping the future of DAs.

The initial concept of Bitcoin is generally at odds with regulation and government control, continuing a cyber-libertarian tradition that can be traced back to at least John Perry Barlow's 1996 "Declaration of the Independence of Cyberspace," which rejected governmental supervision of online communication. However, despite early beliefs that Bitcoin's decentralization rendered it immune to regulation, it now seems there is significant potential for regulatory oversight and situations where such intervention could be beneficial Böhme et al. (2015).

2.2.1 Regulatory Landscape

This section provides an overview of the regulatory landscape.

1. Jurisdictional Approaches:

- Strict Regulatory Environments: Examination of jurisdictions with stringent regulations, such as the United States, where DAs are subject to various regulatory bodies, including the SEC, CFTC, and FinCEN, depending on their classification and use.
- Lenient Regulatory Frameworks: Analysis of jurisdictions with more accommodating regulatory environments, such as Switzerland and Malta, which have adopted clear and supportive frameworks for DA businesses and innovation.
- Regulatory Arbitrage: Discussion of the phenomenon of regulatory arbitrage, where DA businesses and projects may relocate to jurisdictions with more favorable regulatory conditions to continue their operations.

2. Regulatory Classifications:

   - Securities: Analysis of DAs classified as securities, such as initial coin offerings (ICOs) and security tokens, which are subject to securities regulations, including registration, disclosure, and reporting requirements.
   - Commodities: Examination of DAs that are treated as commodities, such as BTC and ETH, which fall under the purview of commodity regulators and are subject to relevant rules and regulations.
   - Currencies: Discussion of DAs that are considered currencies, including stablecoins and CBDCs, and their regulatory implications for businesses and users.

3. Key Regulatory Developments:

   - Financial Action Task Force (FATF): Overview of FATF guidelines and recommendations for DAs, including the Travel Rule, which requires virtual asset service providers (VASPs) to collect and transmit customer information during transactions.

- European Union's MiCA Regulation: Examination of the proposed MiCA regulation, which aims to create a comprehensive regulatory framework for DAs in the European Union, including requirements for issuers, operators, and service providers.
- US Securities and Exchange Commission (SEC): Analysis of key SEC actions and guidance related to DAs, such as the DAO Report, enforcement actions against ICOs, and the treatment of DA exchanges and broker-dealers.

Table 2 presents the regulatory approach to DAs.

Table 2: Comparison of Regulatory Approaches in Different Jurisdictions

Jurisdiction	**Regulatory Approach**	**Key Regulations**
United States	Strict Regulatory Environment	SEC, CFTC, FinCEN
Switzerland	Lenient Regulatory Framework	FINMA, Swiss DLT Law
Malta	Lenient Regulatory Framework	MDIA, VFA Act
European Union	Harmonized Framework	MiCA, AMLD5
China	Strict Regulatory Environment	PBOC, MIIT

Understanding the technical aspects of the regulatory landscape is crucial for DA businesses, investors, and users to navigate the complex and dynamic regulatory environment. The way that DAs are regulated varies greatly from nation to nation, and this creates regulatory risks.

The potential for DAs to be used in illegal activities including money laundering, terrorism financing, and tax evasion is one of the key worries. As a result, KYC and AML rules for DA exchanges and other service providers have been implemented in numerous nations.

Investor protection, market integrity, and financial stability are further regulatory issues that need to be addressed. While some nations have chosen a more laissez-faire attitude, some have imposed licensing and registration procedures for enterprises dealing in DAs.

A tendency toward more governmental monitoring of DAs has emerged in recent years. For instance, in connection to DAs, the Financial Action Task Force (FATF) has created international standards for AML and KYC. The MiCA regulation is a comprehensive legal framework for virtual assets that has also been proposed by the European Union.

The SEC, the Commodity Futures Trading Commission (CFTC), and the Financial Crimes Enforcement Network (FinCEN) are among the regulatory agencies that oversee DAs in the United States. While the CFTC has adopted a more commodities-based approach, the SEC has treated many DAs as securities. These authorities have adopted various ways to regulating DAs.

2.2.2 DAs Adoption

The adoption of DAs has grown significantly in recent years, with various stakeholders, including institutional investors, retail investors, and industries, increasingly incorporating DAs into their operations and investment portfolios.

1. Institutional Adoption:

   - Custody Solutions: Development and implementation of secure and compliant custody solutions, including multi-signature wallets and hardware security modules (HSMs), enabling traditional financial institutions to hold and manage DAs for their clients.
   - Trading and Execution: Integration of DA trading into existing trading platforms and the creation of new institutional-grade platforms, leveraging algorithms and smart order routing to optimize execution and manage risk.
   - Risk Management: Implementation of advanced risk management techniques and tools, such as Value-at-Risk (VaR) models, stress testing, and portfolio optimization, to assess and manage the unique risks associated with DAs.
   - Asset Tokenization: The tokenization of traditional assets, such as stocks, bonds, and real estate, enabling fractional ownership, enhanced liquidity, and improved access for investors.

2. Retail Adoption:

   - Exchanges and Brokerages: Development of user-friendly and secure platforms for retail investors to buy, sell, and trade DAs, incorporating features such as two-factor authentication (2FA), insurance, and fiat on-ramps.
   - Wallets and Storage: Creation of various wallet solutions, including hardware, software, and mobile wallets, with a focus on user experience, security, and compatibility with multiple DAs.
   - Payment Solutions: Integration of DAs into payment systems, allowing users to transact with DAs for everyday purchases, remittances, and cross-border payments, leveraging technologies such as the Lightning Network and stablecoins.
   - Financial Services: Development of DA-based financial products and services, such as lending, staking, and yield farming, enabling users to generate returns on their DA holdings.

3. Use Cases and Industry Applications:

   - Supply Chain Management: Leveraging blockchain technology to improve supply chain transparency, traceability, and efficiency, by creating a tamper-proof record of product provenance and transactions.
   - Identity Management: Utilization of DAs and blockchain technology for secure and decentralized identity management solutions, enabling users to control their personal data and access services more easily.
   - DeFi: Development and growth of DeFi platforms and protocols, offering decentralized financial services, such as lending, borrowing, insurance, and derivatives, powered by DAs and smart contracts.
   - Digital Collectibles and NFTs: The emergence of digital collectibles and NFTs, enabling the tokenization of unique digital and physical assets, with applications in art, gaming, and other industries.

2.2.3 MiCA Regulation

The Markets in Cryptoassets (MiCA) Regulation is the EU regulation that regulates the issuers of stablecoins, which have two types: asset reference stable coins and electronic money stablecoins, and then all the rest of the kinds of crypto assets. Adopted on April 20, 2023, by the European Parliament, MiCA is the first and only legislation of its kind in the world and leads the way for other jurisdictions. MiCA initially was very much focused on stablecoins due to the Libra project, which prompted regulators into action. MiCA establishes and defines a taxonomy of assets from which it will be clear how to distinguish between them. Also, it regulates the crypto asset service providers and provides trading platform services, and investment advisory services around the crypto assets.

Finally, we have a bunch of market integrity provisions that basically ensure that there are levels of market abuse, rules against market manipulation, insider dealing, among others. Published in July 2023, MiCA is implemented in two phases: a 12-month phase-in period for the part of MiCA that deals with stablecoins and then an 18-month implementation period for the rest of MiCA.

Obviously, MiCA is the first, and it's going to be the benchmark. It will be interesting to watch how the baseline ends up being for all the countries, how that's implemented, and any differences that some countries have with their more stringent requirements.

2.2.4 Navigating the Complexities of Compliance

The new risks created by FinTech can be addressed by new approaches to regulation (sometimes termed "Smart Regulation") paired with regulatory and supervisory technologies (collectively referred to as "RegTech"). The term "RegTech," which combines the terms "regulatory" and "technology," refers to the use of technology, particularly information technology ("IT"), for compliance, monitoring, reporting, and regulation. RegTech was first developed to use cutting-edge technology to address regulatory issues in the financial industry. It can facilitate automated data processing within intermediaries as well as between intermediaries and supervisors, large-scale technical management of data, and advanced data analysis. Examples of RegTech include algorithm-based reviews of trading patterns in listed stocks to ensure compliance with insider dealing laws, electronic KYC systems that make it easier for financial intermediaries to onboard clients while also enhancing market integrity, and 31 automated compliance monitoring and reporting with regard to trading limits.

In the European Union (EU), DAs, including CCs, are subject to the same AML and CTF compliance, taxation, and reporting obligations as traditional financial instruments. For VASPs doing business in the EU, the Fifth Anti-Money Laundering Directive (5AMLD), which went into force in January 2020, imposed special restrictions.

VASPs must abide by AML and CTF requirements, including customer due diligence, transaction monitoring, and suspicious activity reporting, as they are deemed "obliged entities" under 5AMLD. Additionally, the legislation mandates that member states control VASPs and make sure they are governed by AML and CTF laws.

Moreover, the 5AMLD mandates that member nations create national databases of beneficial ownership data

for corporations and trusts. By fostering greater transparency on the ownership and management of legal entities, this information can aid in the fight against money laundering and the financing of terrorism.

Since January 2018, a new financial directive has been in place in Europe (MiFID II), regulating financial products and relevant operations.

2.2.5 Challenges and Opportunities in Regulation

This section provides a technical overview of the key challenges and opportunities in the regulation of DAs.

1. Balancing Innovation and Risk:

   - Protecting Consumers and Investors: Developing regulations that safeguard the interests of consumers and investors by addressing risks such as fraud, market manipulation, and cyber-attacks, without stifling innovation in the DA space.
   - Ensuring Market Integrity: Establishing rules and standards to ensure fair and transparent markets, including market surveillance tools and mechanisms to detect and prevent manipulative trading practices and other forms of misconduct.
   - Promoting Financial Stability: Assessing and addressing the potential systemic risks posed by DAs, such as the impact on monetary policy, financial stability, and the traditional banking sector.

2. Global Regulatory Coordination:

   - Harmonization of Rules and Standards: Working towards a consistent and harmonized set of rules and standards across jurisdictions, reducing the potential for regulatory arbitrage and fostering a level playing field for DA businesses and users.
   - Cross-Border Cooperation: Enhancing cross-border collaboration and information sharing among regulatory bodies to effectively supervise and regulate DA activities and service providers operating across multiple jurisdictions.
   - Capacity Building and Technical Assistance: Providing support and technical assistance to help regulators in developing countries build their capacity to regulate DAs effectively, ensuring that they are not left behind in the DA revolution.

3. Regulatory Sandboxes and Innovation Hubs:

   - Fostering a Supportive Environment: Establishing regulatory sandboxes and innovation hubs to provide a controlled environment for DA businesses and projects to test and develop innovative products and services under the guidance of regulators.
   - Streamlining Regulatory Processes: Simplifying and streamlining regulatory processes, such as licensing and registration, to reduce the barriers to entry and support the growth of DA businesses and innovation.

- Continuous Learning and Adaptation: Facilitating a feedback loop between regulators and market participants, enabling regulators to learn from the experiences in the sandbox and adapt their regulatory approaches to keep pace with technological advancements.

2.3 Market Risks

2.3.1 Volatility and downside risk

DAs are a unique asset class that presents investors with opportunities and risks that are contingent upon their particular characteristics such as volatility, type, and profile, among other factors. Among DAs, CCs have emerged as the most liquid asset class, holding this distinction for almost a decade. However, while CCs offer a high level of liquidity, investors must be aware of the potential risks and rewards associated with investing in this asset class and should conduct a thorough evaluation before making any investment decisions. We, therefore, concentrate on CCs and analyze their evolution in terms of their tail event properties. The tail properties of the Profit and Loss (P&L) determine the risk structure of CC-based portfolios which is conveniently determined via Spectral Risk Measures (SRM). Here we provide a brief introduction SRMs and explore their links to investors' preferences. All quantlets are available via quantlet.com and instructive educational elements are available on quantinar.com

The exponential SRM and power SRM, as introduced by Dowd et al. (2008), are commonly cited examples in the field. However, these models have been found to possess certain properties that can pose challenges when applied to practical risk management. Despite these limitations, it has been demonstrated that the exponential utility function may be a viable option under certain circumstances, as originally proposed by Buhlmann (Bühlmann (1980)). However, the choice of a utility function and the determination of the risk aversion parameter depend on the specific financial problem at hand. In this study, the weights for portfolio allocation of CCs are computed by minimizing quantile risk measures, including VaR, ES, exponential SRM, and power SRM.

The empirical evidence can be summarized as follows. First, when attempting to estimate the total value of portfolios, as we observe, during the pandemic the returns of portfolios experiencing higher volatility reach more extreme values. Additionally, after analyzing the performance of Minimum Exponential SRM portfolios across a range of parameters (from 1 to 25), it is found that the portfolios with a parameter value of $k = 1$ (representing the least risk-averse portfolio) demonstrated higher volatility in terms of their cumulative wealth. Conversely, the portfolio with a parameter value of $k = 20$ (representing the most risk-averse portfolio) exhibits the best performance. Second, power SRM is estimated by considering two situations. Based on our analysis, it can be inferred that as the SRM values estimated from these two situations decrease, the corresponding Turnover also decreases. This implies that a strategy with lower turnover is less susceptible to the impact of transaction costs and is more likely to achieve better performance.

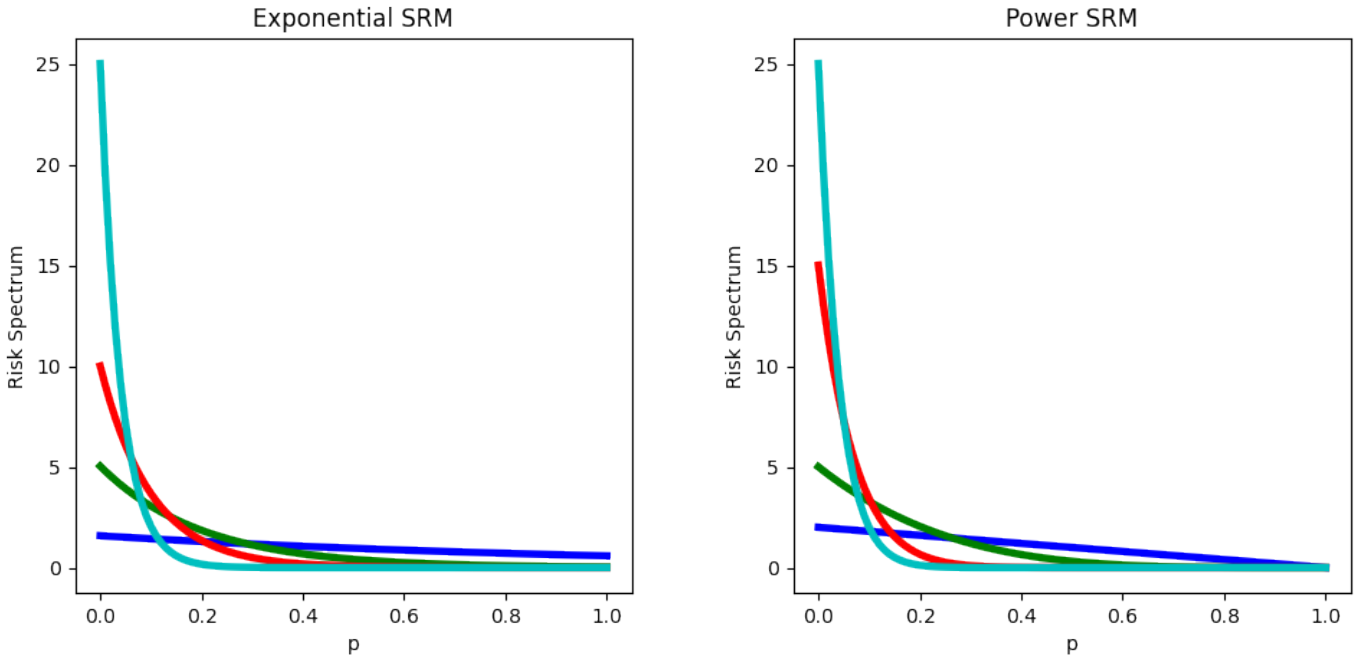

Figure 3: The risk spectra for different SRMs. Left: k =**1**, **5**, **10**, **25**; Right: γ = **2**, **5**, **15**, **25** https://github.com/QuantLet/SRMforDA/tree/main/SRMforDA_RiskSpectrum

2.3.2 Risk contagion

An issue of major practical and academic importance is the investigation of the dependence structure of digital securities. This issue is also linked to the opportunities presented for diversifying market risk. Admittedly, investors in CCs have witnessed high levels of volatility and successive periods of drawdown, the most notable being the recent 2021 crash. A beam of empirical studies investigates the extent to which volatility and extreme risk are transmitted across all types of virtual coins.

Kwapień et al. (2021) look into the cross-correlation structure of returns on a rich panel of 80 CCs traded on the Binance platform. By calculating q-dependent detrended cross-correlation coefficients and analyzing the spectral properties of the correlation matrix, the authors conclude that the CC market has become more compact and coherent over time. Returns on virtual coins exhibit a stronger correlation during periods of economic turmoil, as were the years immediately following the outbreak of the COVID-19 pandemic, and become more independent during times of relative stability. Agyei et al. (2022) employ wavelet techniques to study synchronous and asynchronous linkages between the commonality in virtual coin returns and the CC volatility index (VCRIX). By definition, VCRIX is a forward-looking measure and thus an indicator of the investors' perception of uncertainty about CC market developments. The authors use a comprehensive set of daily data from August 2017 to August 2021 covering global events of major impact, such as the China-US trade war and the COVID-19 pandemic outbreak. Empirical findings suggest a strong linkage between CCs and VCRIX across various investment horizons. The study also finds a significant correlation between Bitcoin and other virtual coins, indicating limited opportunities for diversifying away the Bitcoin market risk within a portfolio that holds shares across various types

of CCs. A great deal of volatility in CC markets seems to be of non-systematic origin not driven by the course of VCRIX. This suggests that while investing in individual CCs can be a risky business, a diverse portfolio of CCs may be able to offer better control of risk in particular market regimes. James and Menzies (2022) explore the relationship between collective dynamics, market size, returns, and volatility in the CC market over time. The authors find that CC prices become more integrated in bearish market regimes, with the level of intercorrelations being significantly lower in periods of market rebound. Additionally, there seems to be a positive relationship between volatility and market size in the sense that the levels of volatility are comparable between CCs of similar market sizes.

At this point, it is important to acknowledge the fact that nowadays CCs are hardly the main investment vehicle of most fund managers. In most cases, they stand as an ingredient of larger portfolios with a high representation of traditional types of financial securities, such as stocks, bonds, FX, and commodities. Financial literature seems to conclude that over the years it is becoming harder and harder for international investors to diversify away the risk of common securities in a properly selected portfolio. This is because returns on these securities tend to be highly correlated, especially in turbulent market periods. Still, if virtual coins occasionally stray from traditional asset classes they can improve the risk-return trade-off of international investors in a well-diversified portfolio.

This issue has been investigated in a number of studies. BenSaïda (2023) look into the link between the exchange rate of Bitcoin and government currencies in a large panel of countries (both developed and emerging). The results from the application of a copula methodology suggest a time-varying dependence structure whereby cross-market linkages increase during periods of economic downturn or turbulence in the market for virtual coins. The authors note that the coupling has been very strong during the recent crises (the 2021 Bitcoin crash and the 2022 Russian – Ukraine conflict) signifying a major alignment of virtual and government currencies. Another example of an application of copula techniques in the investigation of tail dependencies in CCs is Charfeddine et al. (2020). This study focuses on the relationship between Bitcoin and Ethereum with traditional financial assets with a view to quantifying the diversification benefits. Empirical findings indicate a relatively loose (time-varying) dependence structure between the aforementioned CCs and traditional financial securities, which in some periods creates opportunities for risk diversification.

Pele et al. (2021) investigate the commonality of virtual coins and conventional investment asset classes, such as stocks, bonds, real estate, and commodities. By deploying dimensionality reduction and classification methods, they identify three factors that jointly drive daily log returns on the examined panel of assets, termed as a tail factor, memory factor, and moment factor. CCs have exceptionally high exposure to the tail factor, a feature that differentiates them from classical investment assets. They also exhibit a high degree of coherence as an asset class, in the sense that from time to time they group and stray from classical assets. Ahn (2022) elaborate on extreme comovements between CC and equity returns. Following a model-free approach, the researchers find strong left-tail dependence between returns on major CCs (Bitcoin, Ethereum, and BNB) and the S&P 5000 index. In a similar context, Jiang et al. (2021) examine the potential of six major CCs to serve as adequate diversifiers for six large-

capitalization stock indices. Adopting a quantile coherency approach, they show that returns on CCs are typically positively dependent with stock index variations, CCs, and equity markets are more aligned in the medium and long-run, particularly in periods of stock market downturn.

The two aforementioned studies raise a cautionary note against the limited opportunities for risk diversification offered by virtual coins, especially during periods of equity market decline. Maghyereh and Abdoh (2020) explore Bitcoin market linkages with a wider spectrum of security classes, including stocks, bonds, currencies, and commodities. They employ nonparametric econometric techniques (quantile cross-spectral dependence) to uncover possible asymmetries in the dependence structure. Their analysis is supportive of correlation levels changing with the investment horizon and market regime. The authors identify significant long-term dependencies between Bitcoins and the S&P 500 but a weaker linkage with the USD-EUR exchange rate. They also go deeper in terms of investigating the direction of causality and shock contagion between the various asset classes. Their results suggest that variations in conventional asset prices Granger cause Bitcoin returns in lower quantiles, although the inverse direction of causality is generally not observed.

It is found that for CCs the contagion in volatility is stronger between themselves than with risk indices, such as Volatility Uncertainty Index (VIX), Crude Oil Volatility Index (OVX), Economic Policy Uncertainty Index (EPU) or Geopolitical Risk Index (GPR) Al-Yahyaee et al. (2019). Dong et al. (2022) show that most of the anomalies observed in the CC market intensifies in times of low liquidity. Thus, the market becomes very vulnerable in low-liquidity periods.

There is ample literature evidence on the market risk profile of DAs and how this is compared to the investment characteristics of standard asset classes. Literature seems conclusive as to the level of integration between the various virtual coins. Risk contagion among CCs is so prominent that the opportunities for diversifying away coin-specific risk in a portfolio rich in crypto-assets are limited. Intercorrelations become especially strong in bearish market regimes, indicating that in such distressed conditions, investors should make use of derivatives and other hedging instruments available within the virtual-coin asset ecosystem to control their overall risk exposure. Of course, the low liquidity of such instruments and other market frictions (e.g. transaction costs and margin requirements) could pose a limit to the effectiveness of these hedging strategies, an area where regulating authorities could play a decisive role with the adoption of proper measures.

The literature provides mixed evidence as to the level of coupling between returns on virtual coins and other classes of financial securities. The correlation structure is asymmetric; in a bullish economy, DA prices are mainly driven by class-specific news and events, but in periods of market turbulence, their returns are “overshadowed" by the downtrend of the principal market indices. In light of this empirically validated property (also known in the literature as left tail dependence), a global diversification strategy (allocating capital across asset classes and countries) could be of little use in diversifying away shocks emerging from the DA market. It is even more questionable whether DAs could constitute a valuable add-on to the portfolio of institutional investors helping them to improve the risk-return profile of traditional asset classes, especially in periods when they fail to deliver.

(GSCs) pose heightened risks to financial stability due to their cross-jurisdictional reach and potential for mass adoption. These risks are amplified if GSCs become a significant store of wealth, causing volatility in systemic payment and settlement systems (IMF and FSB, 2023).

2.3.3 Volatility and extreme events

One of the major critiques of CCs as a payment device is the characteristic high volatility compared with fiat currencies. For example, as the EUR/USD annual volatility is a mere 10 to 15%, Bitcoin volatility may rise to several hundred % annually, which is not compatible with the requirement of a currency as a store of value. However, several papers have shown that the long-term trend of crypto volatility is decreasing, in particular those cryptos that attain higher market dissemination and capitalization. On the other hand, it is the best investment in the last ten years.

A related problem is the occurrence of extreme events, or large shocks that are much more likely for DAs than for classical assets. Market risk measures such as Value-at-Risk or expected shortfall inevitably increase due to the fat tails of the return distributions, and especially so in periods of high volatility. Moreover, in times of high market turbulence, both volatilities and correlations between cryptos increase, such that the diversification benefits of portfolios break down. Hence, to control market risks, one needs adequate dynamic measures of volatilities and dependencies (linear and non-linear) between DAs.

For NFTs it is difficult a priori to assess market risks as the assets are heterogenous, and one first needs to create an index that represents the market, or a market segment, such as the DAI index of Lin et al. (2022). Based on the index one can then apply standard methods to evaluate volatility, correlation with other markets, and obtain risk measures.

2.4 Liquidity Risk and Market Stability

Market liquidity is one of the key ingredients in mature financial markets that market participants, regulators, and supervising authorities pay close attention to. As Borio (2000) mentions, it is much like systemic risk; both are more easily recognized than defined. The literature such as P2P lending or pool lending in DeFi distinguishes between theoretical and empirical evidence of illiquidity. Illiquidity is carried by underlying market imperfections, such as participation costs, transaction costs, asymmetric information, imperfect competition, funding constraints, and search. We address three questions in the context of each imperfection:

1. How to measure illiquidity

2. How illiquidity relates to underlying market imperfections and other asset characteristics

3. How illiquidity affects expected asset returns (for details, see Vayanos and Wang (2012)).

Vayanos and Wang (2013) provide theoretical and empirical evidence of market liquidity through a study that addresses three main questions: how to assess illiquidity, how it relates to market flaws and other asset

characteristics, and how it impacts predicted asset returns. Even in normal times, asset class liquidity may vary. Low-liquidity financial assets have greater liquidity risk premia, higher transaction costs, and wider bid-ask spreads. Post-crisis changes improved liquidity risk premia pricing, reducing the possibility of fast growth in instruments with unclear hazards. The paper shows where a shortage of liquidity for particular asset classes may overshadow the advantages of new market developments for financial market end-users.

The levels that distinguish the tightness, depth, immediacy, and resiliency of a financial market, all aspects of market liquidity are hard to define. In a quote-driven market, tightness is the bid-ask spread. Depth refers to transaction size that does not affect pricing. Immediacy is the speed at which orders are processed, while resilience is how quickly prices recover to "normal" following order imbalances. Market players, central banks, and supervisory agencies are paying more attention to market liquidity for two reasons. The first concerns long-term financial system evolution; the second concerns current developments. As stewards of monetary and financial stability, central banks are increasingly concerned about market liquidity, since it has become more important for monetary stability as market-oriented operational processes and asset prices dictate policy. Asset prices incorporate market participants' risk assessments and pricing, so central banks and regulatory bodies are using them to monitor financial system vulnerabilities. Recent policies have focused on market discipline, which is supported by this evidence. As financial institutions increasingly rely on markets for risk management, robust market liquidity under stress has become critical and increasingly influenced by risk management practices.

Market players, central banks, and regulatory and supervisory bodies are focusing on market liquidity for two reasons. The first addresses long-term financial system development, whereas the second concerns current events. Since the 1970s, rapid financial market growth has shaped financial systems. Market liquidity is becoming more important for monetary stability due to market-oriented operational processes and asset prices as policy guides. Central banks and supervisors utilize asset prices since they show how market players evaluate risks. This information's validity aids market discipline, which current policymakers have prioritized. As financial institutions increasingly rely on markets for risk management, robust market liquidity during times of stress is crucial and increasingly influenced by risk management practices.

It is crucial to learn about market liquidity from past market volatility. This, of course, is possible in a somewhat stable stochastic scheme. The first lesson is that liquidity considerations fluctuate in relevance in normal and stressed situations. Under great hardship, counterparty dangers and liquidity restrictions might be first-order issues, unlike normal for three reasons; First, trading may create large, if ephemeral, credit exposures, making counterparty risk a factor in transacting. The settlement creates credit exposures. They are caused by the lack of synchronization between the payment and delivery legs of securities and foreign exchange transactions (e.g., the Herstatt risk), the financing needed to meet delivery-versus-payment trades, and, to a lesser extent, the lags between trading and settlement dates. Derivatives agreements include counterparty risk since market prices may greatly affect exposure. Derivatives first managed market risk. Credit risks from transactions with positive market value for counterparties were neglected. Pyramiding transactions to acquire or minimize holdings

sometimes increase credit risks. Second, trading may create opaque exposures and risk profiles. Complex trading tactics and information obsolescence cause opaqueness. Finally, securities and derivatives markets need financial liquidity. Settlement mitigates counterparty risk for economic actors. Trading creates huge settlement volumes that must be funded.

While focusing on liquidity investors are interested in obtaining simple liquidity measures based on daily data. Such attempts were conducted on the stock markets and ended up with several highly recommended measures such as Amihud volatility Amihud (2002), Kyle and Obizhaeva estimator Kyle and Obizhaeva (2016), effective spread estimator of Corwin and Schultz Corwin and Schultz (2012) or the measure of Abdi and Ranaldo Abdi and Ranaldo (2017). Brauneis et al. (2021) indicate that the first two proxies outperform other when estimating liquidity levels, while the Corwin and Schultz (2012) and Abdi and Ranaldo (2017) outperform other measures in describing time-series variations. The latter measures require four prices high-low-open-close, HLOC, while the former is the closing prices and volumes. Even in the situation of single data deficiencies for volume, researchers rely mainly on Amihud illiquidity Long et al. (2022). However, the main problem signaled by Brauneis et al. (2021) is the lack of liability of data offered by some CC exchanges.

The crypto market has grown considerably in recent years in terms of total market value and the variety of new tokens available to investors, however, it poses significant challenges to market participants and regulators, especially after the collapse of the Luna and Terra tokens and the demise of a number of crypto-asset hedge funds, about the risks that DAs create in the financial system. Regulators, in response to those risks, have issued proposals in support of regulatory reforms with the aim of understanding and mitigating the downside risks of holding DAs (regulators include the MiCA Regulation, the Financial Stability Board (FSB), the U.S. SEC, and the Basel Committee on Banking Supervision (BCBS), among others).

Market liquidity is important in international financial markets and the banking system across the world, especially during periods of increased market uncertainty. Liquidity can evaporate quickly in times of stress and lead to increased systemic risk in the financial system. The liquidity risk of DAs has been put under the microscope in recent years. Increased liquidity of DAs lowers investment risk and volatility, reduces transaction costs, and assists in a well-functioning secondary market for those assets which is less susceptible to market manipulation by speculators.

Although the crypto asset market remains relatively small compared to the size of the global financial system, and banks' exposures to crypto assets are of relatively small amounts, it has the potential to raise financial stability concerns and substantial risks for banking institutions (a discussion is provided in the Bank for International Settlements (BIS) Discussion Paper "Designing a prudential treatment for crypto-assets", BCBS, March 2020 https://www.bis.org/bcbs/publ/d490.pdf. Liquidity risk is the risk that a bank's financial safety is negatively affected by its inability to meet its obligations, and has been recognized as one of the top risks a bank faces and as a supervisory priority, especially after the 2007/08 financial crisis.

There are currently different supervision regiments in the EU compared to the U.S. In the U.S. the SEC aims to

enforce existing securities laws for all types of DAs, while the EU takes a different approach. The MiCA regulation was recently ratified by the European Parliament and constitutes an important piece in the digital finance regulation of the EU. It will be in force across all EU's Member States and it is envisaged that it will affect international developments, including in the United States. MiCA has addressed bank liquidity risks related to crypto assets. It lays out definitions for stablecoins, namely Electronic Money Tokens (EMTs) and Asset-Referenced Tokens (ARTs) that are governed by different rules and regulations.

Specifically, ART issuers should maintain a reserve of assets that is clearly separated from the issuer's estate and the reserve of assets of other tokens, in order to manage effectively the liquidity risks associated with the permanent redemption rights of ART holders. Reserve assets should be invested in highly liquid financial instruments with low market and credit risk. Along these lines, ART issuers should perform periodic stress tests under various extreme scenarios that include both financial and non-financial risks. Depending on the stress-test results, EU national authorities may ask ART issuers to hold their own funds (between 20% and 40%) in excess of the amount of funds required under normal conditions. Further liquidity requirements may be specified by the European Central Bank, the European Securities and Markets Authority (ESMA), and the European Banking Authority (EBA). With regard to EMTs, EMT issuers must also have a reserve of highly-liquid assets and fully comply with requirements in relation to liquidity risks, operational risks, and other risks that relate to the mismanagement of reserve assets. Moreover, crypto-asset service providers (CASPs) that provide crypto-asset custody services should keep separate safekeeping accounts for crypto-assets. Those CASPs that are licensed to operate trading platforms, will need to comply with specific liquidity requirements to ensure an orderly and transparent market.

U.S. regulation has also made important steps toward addressing liquidity risk. In February 2023, the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) released a joint statement addressing bank liquidity risks tied to crypto assets. In particular, the following sources of funding from crypto-asset-related entities may pose significant liquidity risk to banking institutions, as the scale and timing of deposit inflows and outflows cannot be predicted with accuracy.

First, the stability of deposits placed by a crypto-asset-related entity may be affected by the behavior of the end customer and not entirely by the crypto-asset-related entity itself. During periods of increased market uncertainty and volatility in the crypto-asset sector, the stability of those deposits may be challenged and can be exacerbated by increased correlations in deposit fluctuations that usually occur during periods of stress. This could potentially lead to bank runs with devastating effects on financial stability. Thus, a liquidity backstop must be introduced that would prevent fire sales of DAs.

Second, deposits that constitute stablecoin-related reserves are exposed to cash outflows emanating from sudden stablecoin redemptions or disruptions in crypto-asset markets. Rapid redemptions of stablecoins driven by factors exogenous to the bank can lead to bank runs, similar to the risk from conventional customer deposits. Bank runs would not only destabilize the DA ecosystem but also disrupt the traditional financial system, as stablecoin issuers

would strive to dispose of their reserve assets to meet redemptions, and such adverse effects would be more severe in the case of less liquid reserve assets, such as commercial paper and corporate bonds (Azar et al., 2022). Liao and Caramichael (2022) argue that a banking framework in which stablecoin issuers are obliged to back their stablecoins with central bank reserves minimizes the risk of runs on stablecoins, although it can reduce credit intermediation. For credit intermediation to remain unaffected, stablecoin deposits must be treated equally with non-stablecoin deposits.

These authorities recognize the need for effective liquidity risk management and propose the following controls are put in place:

- Identify the drivers of potential deposit behavior to determine which deposits are susceptible to volatility
- Assess concentrations or interconnectedness across crypto deposits and their associated liquidity risks
- Incorporate liquidity risks or funding volatility into contingency funding planning, including liquidity stress testing and effective asset-liability risk management practices
- Ensure vigorous due diligence and continued monitoring of crypto-asset-related entities are performed periodically
- Banks should comply with laws and regulations including brokered deposit rules and Call Report filing requirements

Another potential risk for banks is the inability to convert crypto assets into fiat currency at little or no loss, exposing them to liquidity risk. Banks are also susceptible to funding liquidity risk in times of market turbulence in case they issue their own crypto assets.

A number of features of the DA ecosystem are also responsible for vulnerabilities to financial stability. For example, automation may exacerbate operational vulnerabilities – the response time for interventions that could prevent fire sales of assets is reduced when execution of transactions is automated. Moreover, due to the fact that blockchains, crypto-assets, stablecoins, DeFi protocols and centralized exchanges are highly interconnected with each other, there can be spillover effects from one area to another very quickly. The lack of a solid regulatory framework amplifies these vulnerabilities.

In the case of DeFi lending protocols, maturity transformation is facilitated and depositors are allowed to withdraw funds at any time and borrowers to repay their dues at any time. Due to maturity mismatches that may arise, run risk in DeFi may increase. A solution to mitigate that risk is to use varying interest rates on loans and deposits in order to attract deposits, on the one hand, and incentivize loan repayment when liquidity is at low levels, on the other hand. Banks should fully incorporate crypto asset liquidity risk exposures in their overall risk management framework and their capital and liquidity adequacy assessment processes in order to mitigate the risks stemming from crypto assets. Such a framework should include the active involvement of the bank's senior management team.

The liquidity risk treatment for high-risk crypto assets should satisfy the banks' capital and liquidity requirements. Crypto assets are not eligible for inclusion in the Liquidity Coverage Ratio (LCR) and the Net Stable Funding

Ratio (NSFR) as they are not high-quality liquid assets. According to the Bank for International Settlements, crypto assets should be subject to a 0% inflow for the LCR, whilst crypto asset liabilities should be subject to a 100% outflow. With regard to NSFR, crypto assets should be subject to a 100% stable funding factor whilst short-term crypto asset liabilities should be subject to a 0% stable funding factor.

2.5 Socioeconomic Risks

2.5.1 Unequal Access to Digital Financial Services

The gap between individuals who have access to information and communication technologies (ICT) and digital information and those who do not are referred to as generally the "digital divide". Earlier "digital divide" literature recognizes three thematic approaches for the causes and determinants of the digital divide such as access, resources, and forces. Access refers to an individual's access to ICT and his/her ability to make use of ICT in a specific scenario. On the other hand, resources refer to existence of supply of money, materials, infrastructure, social network and other instruments in relation to ICT use. Finally, forces refer to stakeholder groups, systems or institutions which deepen or lessen digital inequality. (Yu et al., 2018) Although the pre-existing "digital divide" has been decreasing significantly in recent years thanks to the swiftly expanding reach and range of internet technologies, today we still need to consider the inequality in terms of having access to digital technologies. Still today socioeconomic factors such as income level, level of education, gender, geographic location, and technological infrastructure contribute to the ongoing digital divide. Specifically, the digital divide exists between urban and rural communities; between high and low-income countries and between the educated and uneducated populations. Individuals who have access only to low-performance computers and/or internet with limited broadband speeds are digitally divided (Du Preez and Le Grange, 2020).

Not only slower internet connection is a concern but still as of 2022, 2.7 billion people-approximately one-third of the world's population- remain unconnected to the internet according to the ITU's Facts and Figures 2022 report (www.itu.int). The digital divide widens even further if only a few type of platforms or certain mobile apps are used to deliver various services. According to the Deloitte 2020 report on "Global Mobile Consumer Trends", the penetration of smartphones has reached 80% and 82%, in developed and developing countries respectively. These figures imply that 20 percent of individuals may not be able to use such services that are only available on smart devices, creating a digital divide. According to very recent data on global market share statistics for smartphones, 71.8 percent of mobiles have the Android operating system and 27.6 percent of users have an iOS operating system developed by Apple. If certain digital services and technologies are primarily provided through only one of these operating systems, a large portion of the global population will not have access to them leading to a "digital divide". Refer to Figure 4 for a visual representation of the global digital divide.

Other studies such as Friedline et al. (2019) also shed some light on digital inequality and digital divide in relation to Fintech and find out that early adopters of Fintech are generally younger people who have digital skills, live in the urban area and have higher income. In a related study, Friedline and Chen (2020) determined

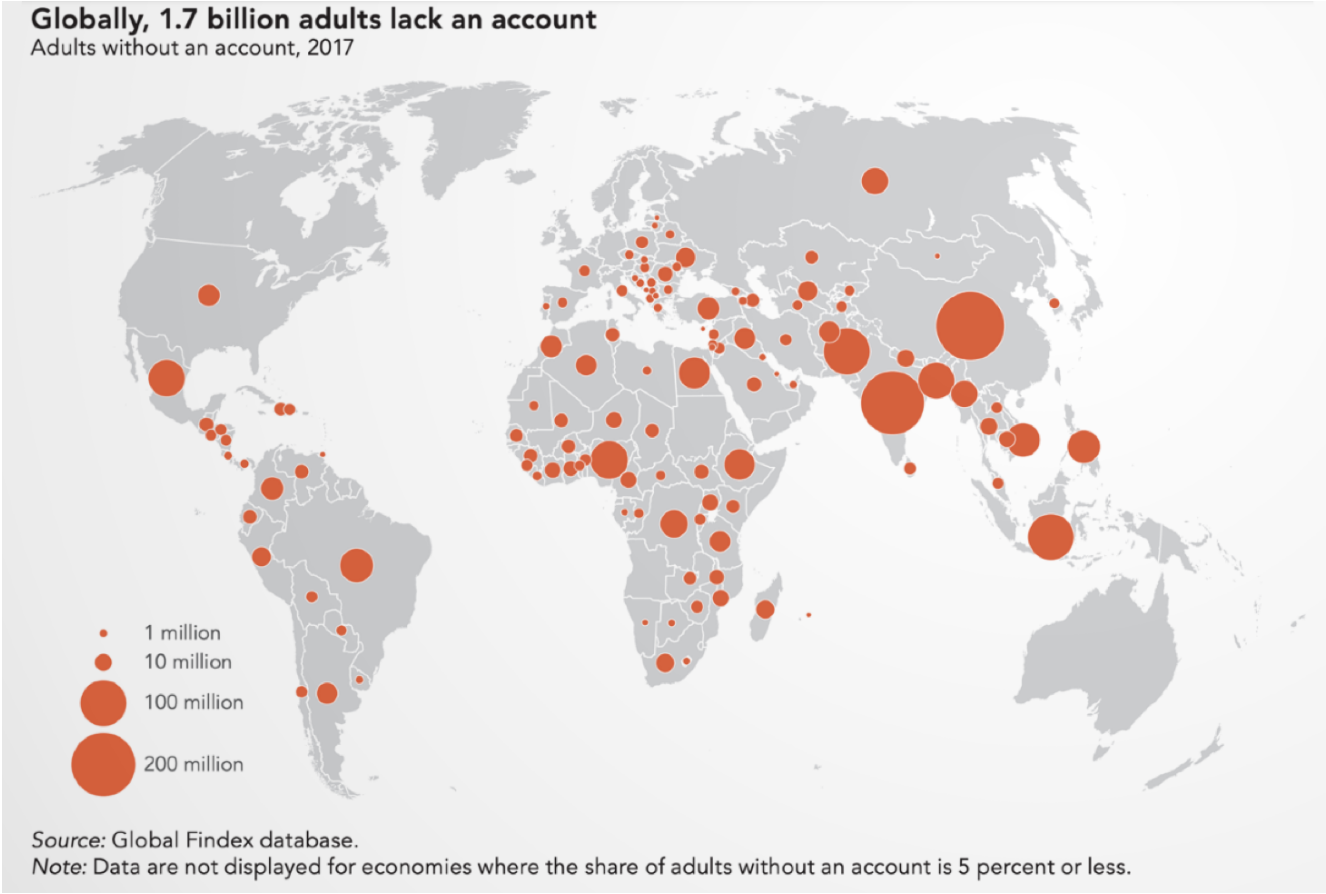

Figure 4: Visual representation of the global digital divide

that communities with higher percentages of black, Latinx, and American Indian/Alaska native populations were associated with decreased usage of Fintech. In addition, communities with higher percentages of black, Latinx, and American Indian/Alaska native populations face decreases in their rates of high-speed internet access. On the contrary, communities with higher percentages of white populations were associated with increased usage of Fintech which is even valid for high-poverty communities. Last but not least, communities with a higher number of residents with a bachelor's degree and higher net worth are more likely to use mobile banking.

These results underline the fact that the phenomenon of the 'digital divide' in relation to Fintech is expected to be more prevalent in high-poverty black and brown communities. The results of Friedline and Chen, (2020) mainly agree with those of Demirguc-Kunt et al. Demirguc-Kunt et al. (2020), who discovered access to digital technology- mobile phone and internet- are likely to be lower among women, poorer adults, those with a lower level of education, and other traditionally disadvantaged groups as well. Here, it is also important to highlight that language might add another barrier and deepen the financial exclusion of underserved populations as digital payment services are mostly offered in English or French. This would prevent the financial inclusion of indigenous and/or minority populations some of which could be illiterate and/or semi-literate (Senyo and Osabutey (2020)).

The results that are discussed above also imply that the reach and the success of fintech services mostly depend on the infrastructure and the mobile technology. Accordingly, the findings of Senyo et al. (Senyo et al. (2022)) also show that cooperative strategies that target collaboration between mobile network operators and fintech companies are needed to ensure financial inclusion and serve the unbanked. The paper provides outstanding examples of fintech

start-ups from Ghana that have leveraged the mobile money platforms of telecommunication operators to reach the unbanked individuals who were already using these mobile operators. Moreover, the paper reports that strategic competition between traditional banks and fintech companies has been observed eventually although traditional banks first showed resistance to fintech start-ups. As traditional banks did not have the strong technology to reach the unbanked population, they realized that they can form strategic partnerships to utilize the digital solutions' of fintech companies in order to financially serve the unbanked population. These kinds of collaborations may benefit society in general as in the case of Ghana and ensure a higher level of financial inclusion.

2.5.2 Regime shifts

Reviewing the market and regulatory environmental conditions in the growth phase is interesting to assess future risks. During the European sovereign debt crisis from 2010-2012 that was triggered by a spill-over from the banking crisis of 2007-2009, the political consensus was to keep low front-end interest rates and offer jointly publicly funded loans to countries that lost their primary market access. In 2015, the ECB started a QE programme to improve the transmission of its monetary policies on the capital market. This programme contributed to suppressing the credit spreads between European countries and lowered also long-term interest rates even to negative territory, but did not succeed in creating inflation for a long time.

The regime shift in interest rates and inflation only came in 2022. Many investors perceived the low-interest rate environment as "financial repression". Unregulated investors became interested in CCs despite their apparent lack of substance because of their unconstrained setup and promise of unhinged exponential growth. The reason for CCs being unregulated for a long time could be that they are labeled as "currencies", which are not regulated as they are issued by central banks of foreign countries, and not as domestic "securities", which are regulated four-fold in most jurisdictions - on the levels of the product, market, distribution and the company level of the financial service providers. A second motivation could be a certain fascination for CCs' technology-based setup and their promise to work in a decentralized way independent from large banks and governments, which resonates well with libertarian minds who don't see the backing of state-issued "fiat money" with taxing power as a valid argument.

Together with the regime shift of rising interest rates in 2022, CC markets increased their correlation to equity markets and fell. This prompted a wave of news on fraud cases like FTX and Terra Luna https://time.com/6243618/crypto-lessons-for-2023/ and on SEC enforcement in the US crypto sector. A BIS study https://www.bis.org/publ/bisbull69.htm shows most retail investors lost money with their crypto investments. In the US, African American lost more on a relative basis than white people https://www.economist.com/graphic-detail/2022/05/20/why-the-crypto-crash-hit-black-americans-hard, https://www.ft.com/content/47d338e2-3d3c-40ce-8a09-abfa25c16a7f.

As a move to gain back some trust, the largest crypto exchanges improved their transparency by offering "proof of reserves" https://www.coalexander.com/post/how-should-binance-prove-it-is-solvent. It is argued

that transparency of reserves can not replace stress testing. The case of the non-digital SVB bank that fell in March 2013 because of a failed ALM concept seems to support this argument. Apart from concerns regarding the solvency of trading platforms and the lack of market supervision, the very lack of substance of many "DAs" that are not tied to another real-world asset or a utility token is still striking. An asset pricing model would deliver a value of zero for the fair value as the sum of discounted cashflows is zero. For many DAs, their "scarcity" seems to be the only marketing argument for its value. Scarcity can of course be technically ensured on the level of a single asset, but the next DA can easily be created, so there is no scarcity in the cross section.

2.6 Environmental Risks

The energy used for calculations and the computational effort creates a substantial carbon footprint for many DAs. Energy used in the process of DA's approval often comes from coal power plants as mining is done at the locations with the cheapest energy worldwide.

There are two main proofing mechanisms for CCs, such as Proof-of-work, PoW, (or mining), and Proof-of-stake (PoS). The former increases energy consumption quite heavily and much more than Proof-of-stake. Thus different coins vary from the point of view of their impact on the environment Jones et al. (2022). One of the examples of response to the environmental damage caused by PoW is the transfer of Ethereum from PoW toward PoS (so-called *The Merge*) Będowska-Sójka and Kliber (2023).

Certain additional actions are already being taken - Wang et al. (2022) proposed the CC Environmental Attention Index, CEAI, based on the headlines indicating risk related to environmental issues. It allows us to measure the awareness of the investors of that kind of risk. The values of the index were almost stable till 2021 when they started to increase. Moreover, the Cambridge Centre for Alternative Finance provides the up-to-date Cambridge Bitcoin Electricity Consumption Index which approximates the daily energy load (University of Cambridge, 2023). As the real electricity load cannot be calculated, they provide the hypothetical range of estimates, from theoretical minimum to theoretical maximum total expenditures on the energy load.

These actions might be better coordinated. The overall monitoring system for energy consumption in the EU should be entered, not only for Bitcoin but also extended to other coins. Last but not least, educational steps should be taken - investors should be aware of the environmental consequences associated with Proof-of-Work currencies.

The environmental exposition is rarely considered in academic papers with respect to portfolio construction and hedging opportunities. Several exceptions could be mentioned: Ren and Lucey (2022) examines the role of PoW versus non-PoW crypto-assets as safe-haven assets against clean energy assets represented by green indices. They find that indices based on clean energy instruments act as a safe haven only for dirty coins. Umar et al. (2022) examine the connectedness between clean or dirty assets and the environmental attention index CEAI. They find that the environmental attention index has a more profound impact on equities than on bonds. Będowska-Sójka and Kliber (2023) find that indices based on clean energy sources are better hedges for oil (a dirty energy source)

than clean or dirty CCs. It is a result of the high volatility of the latter instruments. The energy consumption of ETH has better researched in Woitschig et al. (2023).

3 Mitigating Risks of DAs

To mitigate the risk of cyber-attacks, organizations and countries should invest in robust cybersecurity measures, such as firewalls, antivirus software, intrusion detection and prevention systems, and regular security audits to protect their technical infrastructure.

Developing a response plan is essential to contain and mitigate the breach in the event of a cybersecurity attack. The response plan should include steps to remediate the breach and restore normal operations as quickly as possible. Regularly updating software and hardware is also essential to ensure that they are equipped with the latest security patches and updates.

In addition to these measures, organizations should also consider implementing a security information and event management (SIEM) system. A SIEM system can help organizations detect and respond to security incidents by collecting and analyzing security-related data from various sources. The system can also provide real-time alerts when security incidents occur, enabling organizations to respond quickly and effectively.

Another important measure that organizations should consider is conducting regular security audits. Security audits can help organizations identify vulnerabilities in their systems and processes and take corrective action before a cyber-attack occurs.

Fostering a culture of cybersecurity is essential to ensure that employees are aware of the importance of security and their role in protecting the organization's assets. This culture should encourage employees to report potential security threats and develop a sense of shared responsibility for cybersecurity. To foster this culture, organizations should consider implementing a security awareness training program. The program should cover topics such as password management, phishing scams, social engineering attacks, and other common security threats. The training should be mandatory for all employees and should be conducted regularly to ensure that employees are up-to-date with the latest security threats and best practices.

With AI and machine learning (ML) introduced in all market segments, this technology has revolutionized cybersecurity by enabling automated security systems, NLP, face detection, and automatic threat detection. However, one of the most significant risks associated with AI is adversarial attacks. Adversarial attacks seek to subvert the behavior of AI systems by introducing malicious inputs that can cause the system to malfunction or produce incorrect results. To mitigate the risk of adversarial attacks, researchers are developing new techniques to detect and prevent such attacks. For example, some researchers are developing algorithms that can detect adversarial attacks by analyzing the input data and identifying patterns that are indicative of such attacks. Other researchers are developing new training methods that can make AI systems more robust against adversarial attacks.

3.1 Strengthening Technological Infrastructure

Mitigating DA risks is crucial in today's interconnected and technology-driven world. Here are some strategies to help mitigate risks associated with DAs:

1. Strong Security Measures: Implement robust security measures to protect your DAs. This includes using strong and unique passwords, enabling two-factor authentication (2FA), regularly updating software and applications, and utilizing encryption technologies.

2. Regular Software Updates: Keep your operating systems, applications, and DA management tools up to date. Software updates often include security patches that address known vulnerabilities, reducing the risk of exploitation by hackers or malware.

3. Secure Storage: Choose a secure storage solution for your DAs. Consider using hardware wallets or cold storage options for CCs and digital tokens. These solutions store private keys offline, minimizing the risk of unauthorized access or hacking.

4. Backup and Recovery: Regularly back up your DAs and maintain multiple copies in secure locations. This ensures that you can recover your assets in case of data loss, hardware failure, or other unforeseen events.

5. Education and Awareness: Stay informed about the latest security practices and threats in the DA space. Educate yourself and your team on best practices for online security, phishing attacks, and social engineering techniques. Regularly train employees and users to recognize and avoid potential risks.

6. Due Diligence: Before investing in or transacting with DAs, conduct thorough due diligence. Research the project, team, and underlying technology to assess its legitimacy and potential risks. Be cautious of scams, Ponzi schemes, and fraudulent offerings.

7. Diversification: Avoid putting all your DAs in one place. Diversify your holdings across different types of DAs, platforms, and wallets. This reduces the impact of a single security breach or failure.

8. Secure Communication: Use secure communication channels when discussing sensitive information related to your DAs. Encryption technologies, secure messaging apps, and virtual private networks (VPNs) can help

protect your communications from unauthorized access.

9. Third-Party Risk Assessment: If you use third-party service providers or platforms for managing or trading DAs, conduct a thorough risk assessment. Assess their security measures, track record, and reputation to ensure they meet your standards.

10. Incident Response Plan: Develop an incident response plan to handle security breaches or other DA-related incidents. This plan should outline the steps to be taken, responsible personnel, communication protocols, and recovery processes.

3.2 Security Protocols and Standards

Establishing a security culture is the foundation for any successful security program. Multi-factor authentication should be implemented to ensure that only authorized users access the organization's resources. Encryption should be used to protect sensitive data at rest and in transit. Regular security audits should be conducted to identify vulnerabilities and threats.

Access controls should be implemented to ensure that users only access resources that they are authorized to use. Firewalls and intrusion detection systems should be used to monitor network traffic and detect potential threats. Implementing a disaster recovery plan is essential for minimizing downtime in the event of a security incident.

In addition to these protocols, organizations should also consider adopting advanced security standards such as ISO 27001, NIST Cybersecurity Framework, and PCI DSS. These standards provide a framework for implementing effective security controls and managing risks in the DAs ecosystem.

ISO 27001 is an international standard that provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). The standard specifies requirements for establishing security policies and objectives, conducting risk assessments and risk management processes, and implementing controls to ensure the confidentiality, integrity, and availability of information.

NIST Cybersecurity Framework is a framework developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risk. The framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders.

PCI DSS is a set of security standards developed by major credit card companies to protect against credit card fraud. The standard specifies requirements for securing credit card data during storage, processing, and transmission.

By adopting these protocols and standards, organizations can improve their security posture and reduce the

risk of security threats. Establishing a strong security culture and implementing effective security controls are essential for protecting DAs in the current digital landscape.

3.3 Encouraging Research in Security Solutions

In today's digital landscape, where cyber threats are constantly growing and becoming more intricate, it is of utmost importance to promote the research and development of security solutions. Conducting research can provide invaluable insights from various fields, sectors, and global perspectives, informing the construction, evaluation, and enhancement of digital systems. Moreover, research can drive advancements that enable cybersecurity to keep pace with the ever-evolving landscape of cyber risks. For cybersecurity professionals, research serves as a vital skill to stay updated on new security tools, industry trends, and emerging vulnerabilities. Staying well-informed not only enhances one's desirability to employers but also fosters adaptability across different fields and work environments. To maintain a proactive stance against emerging threats and safeguard technological infrastructure, it is crucial to support research and development in security solutions. The following are some approaches to funding such initiatives:

- Governments can allocate funding to universities, research institutions, and private companies to facilitate research and development of security solutions. These financial resources can expedite the development of innovative security technologies and solutions.
- Collaboration between academic institutions and industry can cultivate knowledge exchange, interdisciplinary research, and practical solution development. Industry can contribute real-world use cases, while academia can provide specialized expertise in security research and development.
- Organizing hackathons and competitions can serve as engaging platforms to stimulate innovation in security solutions. These events bring together developers, researchers, and security experts to collaborate on novel approaches.
- Embracing open-source development can foster innovation and collaboration in security solutions. Open source projects enable community-driven development, leading to faster progress, enhanced security measures, and wider adoption of new technologies.

Promoting collaboration between the public and private sectors is essential for managing risks in the DAs ecosystem. Collaboration can bring together the regulatory oversight and guidance of the public sector and the innovation and expertise of the private sector.

Collaboration between the public and private sectors can take many forms, such as information sharing, joint research and development, and public-private partnerships.

Furthermore, organizations should consider collaborating with others in their industry to share best practices and develop common standards for managing risks in the DAs ecosystem. Collaboration within industries can create a common understanding of risks and foster the development of effective solutions.

By promoting collaboration between the public and private sectors and within industries, organizations can improve their security posture and reduce the risk of security threats. Collaboration can lead to increased information sharing, better coordination of efforts, and the development of more effective solutions for managing risks in the DAs ecosystem.

Public-private partnerships (PPP) have been identified as a critical component of cybersecurity, especially for the protection of critical infrastructure. PPPs can enhance the cyber ecosystem's overall security by enabling effective identification and addressing of vulnerabilities. By sharing information and resources, PPPs can improve cybersecurity and ensure critical infrastructure is better protected against cyber attacks. However, maintaining trust between the public and private sectors is essential, and it is crucial to define roles and goals. PPPs are necessary for improving cybersecurity posture and are a vital part of national cybersecurity strategies. By combining public and private resources, PPPs can offer benefits such as risk sharing, innovation, efficiency, and social impact. However, PPPs also come with challenges and pitfalls that can jeopardize the project's success and stakeholders' interests.

Strengthening technological infrastructure and enhancing cybersecurity in the DAs ecosystem face several challenges. Some of these challenges include:

- complexity, with the increasing complexity of technology, it is becoming harder to keep up with the evolving threats and vulnerabilities;
- lack of skilled workforce, which can make it difficult for organizations to find the right people to secure their systems;
- lack of other resources, including funding, personnel, and technology, to adequately address cybersecurity threats. This can be especially challenging for small businesses and organizations with limited budgets and resources;
- lack of awareness, is one of the greatest obstacles to cybersecurity, as many users, as not aware of the potential risks and vulnerabilities of the devices and systems they use, and they don't take the necessary precautions to protect themselves and their data;
- rapidly evolving technologies, faster than ever before, technology is advancing, making it challenging for enterprises to keep up with the most recent security measures and updates;
- human error, including employees who expose sensitive information or fall victim to a phishing attack, as well as users who accidentally download malware or engage in risky behavior online;
- insider threats, which include employees, contractors, and vendors who intentionally or accidentally leak sensitive information or compromise security.

To overcome these challenges, it is essential to have a comprehensive cybersecurity strategy that includes a mix of technical measures, policies, and training programs to raise awareness and promote best practices. Additionally,

cooperation between stakeholders, including government agencies, private sector companies, and individuals, is critical to addressing cybersecurity threats effectively.

3.4 Bridging the Digital Divide

The development of DAs has been at a fast pace recently. Some of the assets have appeared on the market whereas the regulations were not fully in place. It might have caused uncertainty in the society. Whenever new technology appears in everyday life, it generates multiple questions and challenges for the end users. The process of adaptation might be shortened depending on the actions taken to minimize the uncertainty. As the popularity of DAs is highly connected to the number of users leveraging them, there should be a clear strategy outlining the socioeconomic risks and bridging the digital divide. The challenges have been described below alongside the mitigation plan.

Every time a new DA is implemented, it should be clearly described by its creators. The characterization ought to include the potential use cases, as well as identified challenges. The full range of available services is needed by society for them to decide if they want to leverage it. However, in light of the fast development of new technologies, even the creators of DAs might not be fully aware of their full scope. It should be a joint effort of users and creators to provide the necessary details of the usage. The most frequent potential challenges with the DAs outlined in the literature are the misuse of private data and not enough care for intellectual property Dogru et al. (2018). However, storing the data in a distributed way minimizes potential leakage and improves security. One needs to keep in mind the application of the DA is not the same in every place as socioeconomic conditions have an influence as well.

Even if DAs were created fully correctly for the first time, they would not be leveraged without at least basic knowledge in society on economics and finance. It is especially a challenge in developing economies where the overall knowledge is comparatively smaller than in other ones. In some of those countries, the basics of the financial system may not be fully implemented which is a prerequisite for the right use of more advanced instruments Ogbonna et al. (2020). Introducing DAs facilitates financial inclusion and empowerment. The financial instruments do not exist in a void, it is a highly interconnected system. Some ways of using the assets can be discovered once they are fully tested. The role of institutions in creating public opinion cannot be underestimated. If negative information is presented more frequently, it will not encourage society to even become interested in what DAs might offer, not to mention begin using them. One of the ways how to encourage society is to leverage a platform where users could have some amount of test currency and trade it as if it was real. That way the users get an understanding of how the instruments can be leveraged and incorporate the practical usage into the learned theory.

Some of the benefits of the DAs might be seen as threats. The often-cited advantage of DAs is decentralized decision-making Barrett (2015). It shifts the potential risks from the end user to the unknown body. Some transactions might be scheduled and executed without the fully involved user. For instance, the user can beforehand

establish a specific rule in the system that if the price falls below a set level, the transaction is executed. If multiple users decide to trade this way, it might impact the price of the instrument. Given the fact the transaction is irreversible with the same details, the user might feel they do not fully control the situation.

Once a DA is created or improved, in the beginning, it might not be regulated by the law. The rules are usually secondary to asset creation as first one needs to be fully clear on the potential application. It might be a vicious circle – a person might not want to use the DAs due to not enough regulations and the regulations will not be created without the user. The laws of technology are created for people, not the other way around. The specifics of the DAs do not make it easier for the law to be implemented. One of the examples is smart contracts which have the role of intermediaries. The applicable rules cannot be changed once they are established and implemented. DAs are novel not only in the context of leveraged technology but also from a law perspective. They do not fall into the existing regulations Azar et al. (2022). The process of creating the law is especially complex in countries with multiple layers of institutions. One of the epitome exemplifications is when the EU member country needs to efficiently implement the regulations coming from the EU level, as well as the national specifics. A possible way how to encourage society is to run public consultations and include their voice in law formation. In this way, the general public becomes the prosument, which is a combination of producer and consumer. They have an active part to create the laws and having in mind they will leverage the rules later on, they have an incentive to propose the most effective laws. The key is to ensure privacy and data protection through robust policies.

Summing up, DAs hold a promising light in advancing technology. However, the outlined steps are necessary to fully unblock the full usage and make the most of them. The benefits of leveraging them heavily outweigh the potential drawbacks. The extent of the DAs is increasingly connected with the financial sector. Since the range of potential assets is diversified, one can start using the least complex ones to get awareness. Later on, the scope can be expanded to the more advanced ones. If DAs branches become a consistent part of the financial system, the stability becomes increasingly tangible.

The emergence of behavioral economics has also changed attitudes toward consumer protection, which is particularly important to minimize risks in the DA market. In the case of consumer information problems, traditional economics suggests that, as far as possible, the amount of information available should be increased. The advent of behavioral economics has modified this approach in several respects. For boundedly rational individuals, "more" information is not necessarily always better. It is not only the quantity of information that is important, but also its other ('qualitative') properties (how it is delivered). The behavioral approach places less importance on information in quantitative terms, but the way it is understood, the way it is presented and similar characteristics become important. Cognitive errors can also be made by salespeople; buyers need to be "protected" not only from themselves. Precise regulation of information disclosure places a very heavy burden on regulators, so other forms of regulation should be considered.

The practical implications of the change in theoretical considerations are as follows: it is not realistic to expect that, in the case of a wide range of services, the consumer will become an expert in the field in question, as a result of the complex and inherently unrelated information provided, and will be informed to the same extent as a professional company, thus restoring the equilibrium necessary for rational decision-making. However, this is not in the interest of the consumer (and society) either. Consumers want to buy goods and services that meet their needs. He does not want to understand how the goods or services he buys work but wants to use them for his economic purposes. He wants to enjoy the benefits of using the product safely and would entrust someone else with the task of professionally assessing the conditions for this and ensuring that he does so. In this way, the consumer would be relieved of ineffective information, relieved of considerable responsibility, and save time. This is particularly the case for complex financial services, especially when they are combined with AI applications as part of digital tools that are also considered complex by experts.

Digital tools should be subject to strict rules and obligations on product safety and product liability before they enter the market, and to 'consumer protection by design' along the lines of 'privacy by design', and public authorities should conduct a professionally controlled trial run with market players.

3.5 AI and ML in Risk Mitigation

Automation, AI, ML and cloud technologies are fast becoming essential tools for the financial services industry-not least within asset management and security services. These tools are already used to enhance a variety of processes, from front-office activities to compliance and operations in the back office. They promise to usher into a new age of competitive services and efficient processing based on digital intelligence. However, realizing the transformational potential of these technologies requires advanced planning and preparation. One of the main issues is to train the system properly. If the same training dataset is used for many different tasks, it is likely that the dataset does not accurately reflect the background needed to build the model distorting the effectiveness of the model, leading to erroneous results and discrimination. In general, institutions' interest in using AI and machine learning techniques to improve (credit) risk management practices has grown in recent years, partly due to evidence of the incompleteness of traditional techniques and partly due to the widening digital divide between advanced and developing economies.

There is evidence that credit risk management capabilities can be greatly improved by exploiting AI and machine learning techniques due to their ability to semantically understand unstructured data. Forecasting, Natural Language Processing (NLP) as chatbots, contract reviewing, and report generation, Image recognition, and Anomaly detection represent examples of intersection points at which to assess the added value of collaboration between the approaches (see Aziz and Dowling (2019)). As early as 1994, Altman and colleagues carried out an initial comparative analysis between traditional statistical methods of predicting non-performing and failing loans and an alternative neural network algorithm, concluding that a combined approach of the two significantly improved accuracy (Altman et al. (1994)). Also Machado and Karray (2022) propose the use of different ensemble

and hybrid ML models to predict commercial customers' credit scores. Judging from the levels of the connectedness of virtual coins with standard financial securities, there is a need for the development of multivariate ML paradigms for modeling the correlation structure or the joint distribution of asset returns. These paradigms could be proven of higher practical relevance and better suited to the needs of fund managers compared to statistical methods due to their ability to quantify dependencies on particular quantiles of the joint return distribution and accommodate the evolutionary feature of the dependence structure.

Consequently, the role of AI and ML in risk mitigation is becoming increasingly important. Ways in which AI and ML can help mitigate the risks associated with DAs include:

1. Fraud Detection: AI and ML can analyze large volumes of data to detect patterns of fraudulent activity associated with DAs. This can help financial institutions identify potential risks and prevent fraud before it occurs.

2. Risk Management: AI and ML can also help financial institutions manage the risks associated with DAs. By analyzing transaction data in real time, AI and ML can identify potential risks and alert institutions to take action to mitigate those risks. Applications to operational risk and compliance with risk management regulations clarify its potential. One obvious conclusion is that the time-consuming and costly nature of risk management will diminish significantly. However, it is crucial to consider that the complete automation of processes, from data collection to decision-making, will make the need for human supervision even more pressing to avoid transparency and ethical problems.

   In this context, the standard deviation of unexpected events, often known as volatility, can be used to calculate the market risk (see Jorion (2007), Zihan et al. (2023), Zhang et al. (2017)).

3. Compliance: Compliance with regulations is a critical aspect of managing the risks associated with DAs. AI and ML can help financial institutions ensure compliance by automating regulatory compliance checks and monitoring transactions for suspicious activity. Furthermore, ML solutions may be used for liquidity risk analysis (Tavana et al., 2018; Guerra et al., 2022) and for operational risk analysis.

4. Cybersecurity: The security of DAs is crucial to mitigating risks in the financial ecosystem. AI and ML can help financial institutions identify potential cybersecurity threats and take action to prevent attacks.

   The current literature shows that Conversational AI Chatbots are game-changers for the FinTech industry and customers since they continuously monitor and scan accounts to check for any suspicious activities, i.e., fraud detection. Thus, at the time of any such financial transaction occurrence, chatbots immediately alert the customers (Kallel et al., 2023).

   As the world of CC derivatives evolves at an unprecedented pace, it is proposed to address the obstacles by formulating an index that accurately measures fear through the use of CRIX-based CC options.

5. Market Analysis: AI and ML can contribute to the analysis of market data to provide insights into trends

and patterns related to DAs. This can help financial institutions make informed decisions about investing in DAs and managing their risks. More specifically, the emergence of new AI-based conversational agents (e.g., OpenAI ChatGPT, Microsoft Bing Chatbot, Google Bard, DeepMind Sparrow, etc.) as well as their development and applicability have a significant impact on the Financial and FinTech industry by providing better customer service, reducing costs and increasing efficiency by automating repetitive tasks (Huang and Lee (2022)).User engagement and customer satisfaction (Hsu and Lin (2023)) can also be increased by using AI-based conversational agents in the FinTech industry as it can draw in more clients who want to look and analyze in real-time services or items without any direct human interaction.

One further relevant element that remains to be addressed on the topic is the trasparency referred to the ability to understand how an AI system makes decisions or predictions. The lack of transparency in AI systems can be a major issue, as it can lead to decisions being made without a clear understanding of how they were arrived at. This lack of understanding can be particularly problematic in high-stakes applications such as healthcare, criminal justice, and finance, where incorrect or biased decisions can have serious consequences. An intuitive approach to build a model based on target based clusters to improve credit scoring is available at Teng et al. (2023).

Another approach is to require AI developers to provide detailed documentation of how their systems work, including information about the data used to train the system and the algorithms used to make decisions. Another approach is to develop tools for explaining how an AI system arrived at a particular decision or prediction, such as visualizations or natural language explanations. For example, EU guidelines (European Commission, 2019) outline a set of ethical principles suggesting that AI developers should provide clear documentation of their systems and develop tools for explaining AI decisions. On the other hand, DARPA explainable artificial intelligence (XAI) program (Gunning (2017)) provides information on the agency's efforts to develop AI systems that are transparent and explainable. It discusses some of the challenges involved in achieving these goals and highlights some of the research being done in this area. There has been a growing interest in the research community in the development of XAI systems.

An example is provided by exploiting DA services. Its use can help mitigate risks associated with managing DAs by providing security, compliance, convenience, liquidity, and expertise. Before investing in DAs, it's essential to choose a reputable and trustworthy provider and to carefully consider the risks involved (i.e. NFTs).

Among the example of successful implementation of AI in DAM (DA management):

- *AI keywording with computer vision.* When you have numerous assets in your digital library it can be difficult to properly tag all of them manually. Using AI allows you to bulk tag multiple assets, thus significantly reducing time spent on enterprise metadata management.

- *Face recognition in DAs management.* The user asks AI to scan a given image for faces and detects all faces and highlights in the image. Users assigns a name to the face. DAM then assigns that name to the same face. It had identified across multiple pictures a user can search through their library by that metadata. The benefit

of AI-auto-tagging in DAM is that it is possible to quickly apply metadata to millions of assets without human intervention. This represents a significant improvement to DAM system management as it eradicates one of the major bottlenecks in asset ingest - applying metadata.

AI and ML offer a range of benefits for DAM, including automated tagging, improved searchability, reduced manual labor and human error, optimization of workflows, and enhanced security and compliance. In the future, AI-powered analytics and image generation could further enhance the capabilities of DAM systems. Additionally, the use of AI and ML can help mitigate risks associated with the proliferation of DAs, by analyzing large volumes of data in real time, identifying potential risks, preventing fraud, ensuring compliance with regulations, enhancing cybersecurity, and providing insights into market trends.

In conclusion, the proliferation of DAs has brought about new risks in the global financial ecosystem, but AI and ML can help mitigate these risks. By analyzing large volumes of data in real time, these technologies can identify potential risks, prevent fraud, ensure compliance with regulations, enhance cybersecurity, and provide insights into market trends. As DAs continue to grow in popularity, the role of AI and ML in mitigating risks will become increasingly important.

4 Towards a Resilient and Inclusive DA Ecosystem

The exploration of DAs for the coming digital era is nothing short of revolutionary. In this position paper, we have defined DAS, showed their multifaceted risk profiles and have proposed proactive mitigating elements. As the understanding of DAs deepens and their applications broaden, the need to navigate the risks in a forward looking manner becomes paramount. The a roadmap to mitigate DA risks serves as a guide towards a resilient and inclusive digital asset ecosystem.

It is evident that the digital realm is evolving at a pace beyond what traditional finance and regulatory frameworks were initially designed for. From the primal notion of digital currencies to complex structures like NFTs, CBDCs, and DeFi, the expanse of DAs is vast. Each of these DAs brings along its unique set of challenges and opportunities. The foundational blockchain technology underpinning many DAs has redefined how we trust, pay, and trade.

Risks, especially with emerging technology, are imminent. As the history of technology has shown, with innovation comes vulnerability. However, technological challenges, while daunting, are somewhat predictable and often solvable with further research and development.

On the other hand, legal and regulatory risks are intricate. The regulatory landscape is in flux, continually trying to catch up with the pace of digital innovation. While frameworks like the MiCA regulation provide decision platforms. The complexities of compliance, both for entities and regulators, require harmonized global efforts. Market risks, highlighted by extreme volatility and jumps in sentiment markets and underscore the need for modern financial instruments and infrastructures.

Furthermore, socioeconomic risks emphasize that while DAs promise democratization, they can inadvertently perpetuate existing inequalities. The fear of regimes shifting and unequal access to digital financial services is a stark reminder that the digital divide is real and potent. Lastly, the environmental implications of DAs, especially for BC-based CCs, cannot be understated. As the world grapples with climate change, the DA ecosystem needs to introspect and innovate for sustainability.

Mitigating these risks is not a linear journey but a multi-pronged approach. Strengthening technological infrastructures goes hand in hand with setting security protocols and standards. It's not enough to just design robust systems; ongoing research in security solutions is imperative. Bridging the digital divide, while a broader societal challenge, has specific implications in the DA world. Efforts must be focused on ensuring inclusivity, making sure that DAs don't become another privilege for the few but a right for many. The promise of artificial intelligence (AI) and machine learning (ML) in risk mitigation is also encouraging.

As we move towards a more resilient and inclusive DA ecosystem, it's evident that collaboration is key. Stakeholders, from technologists to regulators, investors to end-users, need to engage in continual dialogue. DAs, in their essence, are decentralized, but their successful, risk-mitigated integration into our world requires a centralized effort of collective intelligence and shared responsibility.

In sum, the DA journey is just beginning. The road ahead is filled with opportunities wrapped in challenges. By recognizing these challenges, understanding their nuances, and innovatively mitigating them, we can ensure that DAs live up to their transformative promise. The future of digital assets is not just about technological brilliance but about creating an ecosystem that is secure, inclusive, and sustainable. The stakes are high, but so are the rewards.

5 Glossary of Key Terms and Concepts

Table 3 lists abbreviations used in this paper.

Table 3: List of Abbreviations and Descriptions

Abbreviation	Description
5AMLD	The Fifth Anti-Money Laundering Directive
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interfaces
ARTs	Asset-Referenced Tokens
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
BPMN	Business Process Modeling Notation standard version 2.0
CBDC	Central Bank Digital Currency
CC	Cryptocurrency
DeFi	Decentralized Finance
DFP	Digital Finance Package
DLT	Distributed Ledger Technology
EBA	European Banking Authority
ECB	European Central Bank
EMTs	Electronic Money Tokens
ERP	Enterprise Resource-Planning System
ESMA	European Securities and Markets Authority
FSB	Financial Stability Board
HSM	Hardware security module
IS	Information System
IT	Information Technology
IT/IS	Information Technology and Information System
KYC	Know Your Customer
MiCA	Markets in Crypto-Assets
ML	Machine Learning
NLP	Natural Language Processing
NFT	Non-Fungible Token

Continued on next page

Table 3 – continued from previous page

Abbreviation	Description
PII	Personal Identifying Information
SEC	Securities and Exchange Commission
SIEM	Security Information and Event Management
VIX	Volatility Uncertainty Index
VASP	virtual asset service provider
XAI	Explainable Artificial Intelligence

6 Acknowledgments

The authors are grateful to working group members and management committee members of the COST (Cooperation in Science and Technology) Action CA19130 Fintech and Artificial Intelligence in Finance. This European network has been created in 2018 and now encompasses more than 280 researchers from 51 countries internationally.

This document is based upon work from COST Action CA19130, supported by COST (European Cooperation in Science and Technology). COST is a funding agency for research and innovation networks. Their Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career, and innovation. The collaboration with the COST Action CA21163 Text functional and other high-dimensional data in econometrics: New models, methods, applications is acknowledged.

Financial support by the Swiss National Science Foundation within the project Mathematics and Fintech - the next revolution in the digital transformation of the Finance industry (IZCNZ0-174853) is gratefully acknowledged. We are also grateful for financial support from the Swiss National Science Foundation under the grant IZSEZ0-211195 (Anomaly and Fraud Detection in Blockchain Networks). The authors also acknowledge financial support from the Swiss National Science Foundation within the project Narrative Digital Finance: a tale of structural breaks, bubbles & market narratives (IZCOZ0-213370). We acknowledge funding from the European Union's Horizon 2020 research and innovation program FIN-TECH: A Financial supervision and Technology compliance training programme under the grant agreement No 825215 (Topic: ICT-35-2018, Type of action: CSA). We also acknowledge funding from the National Science and Technology Council of Taiwan under grant NSTC 112-2118-M-A49-001-MY2.

The Cooperation between ING Group and the University of Twente, in the context of promoting Artificial Intelligence in Finance in the Netherlands and beyond is gratefully acknowledged.

We gratefully acknowledge the support of the Marie Skłodowska-Curie Actions under the European Union's Horizon Europe research and innovation program for the Industrial Doctoral Network on Digital Finance, acronym: DIGITAL, Project No. 101119635. Their significant contribution has been instrumental in advancing our research and fostering collaboration within the digital finance field across Europe.

The paper development was partially supported by project no. TKP2021-NVA-29 that has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme. We also acknowledge the support of IDA, Institute of Digital Assets, RNCRP, C9, 760046/23.05.2023.

References

Abdi, F. and A. Ranaldo (2017, 08). A Simple Estimation of Bid-Ask Spreads from Daily Close, High, and Low Prices. The Review of Financial Studies 30(12), 4437–4480.

Agyei, S. K., A. M. Adam, A. Bossman, O. Asiamah, P. Owusu Junior, R. Asafo-Adjei, and E. Asafo-Adjei (2022). Does volatility in cryptocurrencies drive the interconnectedness between the cryptocurrencies market? insights from wavelets. Cogent Economics & Finance 10(1), 2061682.

Ahn, Y. (2022). Asymmetric tail dependence in cryptocurrency markets: a model-free approach. Finance Research Letters 47, 102746.

Al-Yahyaee, K. H., M. U. Rehman, W. Mensi, and I. M. W. Al-Jarrah (2019). Can uncertainty indices predict bitcoin prices? a revisited analysis using partial and multivariate wavelet approaches. The North American Journal of Economics and Finance 49, 47–56.

Altman, E. I., G. Marco, and F. Varetto (1994). Corporate distress diagnosis: Comparisons using linear discriminant analysis and neural networks (the italian experience). Journal of Banking Finance 18(3), 505–529.

Amihud, Y. (2002). Illiquidity and stock returns: cross-section and time-series effects. Journal of Financial Markets 5(1), 31–56.

Apostolaki, M., A. Zohar, and L. Vanbever (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. In 2017 IEEE Symposium on Security and Privacy (SP), pp. 375–392. IEEE.

Azar, P. D., G. Baughman, F. Carapella, J. Gerszten, A. Lubis, J. P. Perez-Sangimino, C. Scotti, N. Swem, A. Vardoulakis, and D. E. Rappoport W (2022). The financial stability implications of digital assets. FRB of New York Staff Report (1034).

Aziz, S. and M. Dowling (2019). Machine learning and ai for risk management. In Disrupting finance, pp. 33–50. Palgrave Pivot, Cham.

Barrett, S. (2015). Subnational adaptation finance allocation: Comparing decentralized and devolved political institutions in kenya. Global Environmental Politics 15, 118–139.

BenSaïda, A. (2023). The linkage between bitcoin and foreign exchanges in developed and emerging markets. Financial Innovation 9(1), 38.

Borio, C. (2000, 11). Market liquidity and stress: selected issues and policy implications. BIS Quarterly Review.

Brauneis, A., R. Mestel, R. Riordan, and E. Theissen (2021). How to measure the liquidity of cryptocurrency markets? Journal of Banking & Finance 124, 106041.

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

Bühlmann, H. (1980). An economic premium principle. ASTIN Bulletin: The Journal of the IAA 11(1), 52–60.

Będowska-Sójka, B. and A. Kliber (2023). Proof-of-work versus proof-of-stake coins as possible hedges against green and dirty energy. Online access on 9-May-2023.

Charfeddine, L., N. Benlagha, and Y. Maouchi (2020). Investigating the dynamic relationship between cryptocurrencies and conventional assets: Implications for financial investors. Economic Modelling 85, 198–217.

Connolly, L. Y. and D. S. Wall (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security 87, 101568.

Corwin, S. A. and P. Schultz (2012). A simple way to estimate bid-ask spreads from daily high and low prices. The Journal of Finance 67(2), 719–760.

Demirguc-Kunt, A., A. Pedraza, and C. Ruiz-Ortega (2020, August). Banking sector performance during the covid-19 crisis. Policy Research Working Paper 9363, Europe and Central Asia Region, Office of the Chief Economist Development Economics, Development Research Group.

Dogru, T., M. Mody, and C. Leonardi (2018). Blockchain technology & its implications for the hospitality industry. Boston University.

Dong, B., L. Jiang, J. Liu, and Y. Zhu (2022). Liquidity in the cryptocurrency market and commonalities across anomalies. International Review of Financial Analysis 81, 102097.

Douceur, J. R. (2002). The sybil attack. In Peer-to-Peer Systems: First InternationalWorkshop, IPTPS 2002 Cambridge, MA, USA, March 7–8, 2002 Revised Papers 1, pp. 251–260. Springer.

Dowd, K., J. Cotter, and G. Sorwar (2008). Spectral risk measures: properties and limitations. Journal of Financial Services Research 34, 61–75.

Du Preez, P. and L. Le Grange (2020). The covid-19 pandemic, online teaching/learning, the digital divide and epistemological access. Unpublished paper 1, 90–106.

Flick, C. (2022). A critical professional ethical analysis of non-fungible tokens (nfts). Journal of Responsible Technology 12, 100054.

Friedline, T., M. R. Despard, and S. West (2019). Does the composition of financial services in a community relate to an individual's savings account ownership? Journal of Community Practice 27(1), 5–30.

Guerra, P., M. Castelli, and N. Côrte-Real (2022). Machine learning for liquidity risk modelling: A supervisory perspective. 74, 175–187. Publisher: Elsevier.

Gunning, D. (2017). Explainable artificial intelligence (xai). Defense advanced research projects agency (DARPA), nd Web 2(2), 1.

Guo, L., W. K. Härdle, and Y. Tao (2022). A time-varying network for cryptocurrencies. Journal of Business & Economic Statistics, 1–20.

Härdle, W. K., C. R. Harvey, and R. C. Reule (2020). Understanding cryptocurrencies.

Hsu, C.-L. and J. C.-C. Lin (2023). Understanding the user satisfaction and loyalty of customer service chatbots. Journal of Retailing and Consumer Services 71, 103211.

Huang, S. Y. and C.-J. Lee (2022). Predicting continuance intention to fintech chatbot. Computers in Human Behavior 129, 107027.

IMF and FSB (2023). IMF-FSB synthesis paper: Policies for crypto-assets.

James, N. and M. Menzies (2022). Collective correlations, dynamics, and behavioural inconsistencies of the cryptocurrency market over time. Nonlinear Dynamics 107(4), 4001–4017.

Jiang, Y., J. Lie, J. Wang, and J. Mu (2021). Revisiting the roles of cryptocurrencies in stock markets: A quantile coherency perspective. Economic Modelling 95, 21–34.

Jones, B., A. Goodkind, and R. Berrens (2022). Economic estimation of bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold. Scientific Reports 12(14512).

Jorion, P. (2007). Value at risk: the new benchmark for managing financial risk. The McGraw-Hill Companies, Inc.

Judmayer, A., N. Stifter, K. Krombholz, and E. Weippl (2017). History of cryptographic currencies. In Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms, pp. 15–18. Springer.

Kaal, W. A. (2020). Digital asset market evolution. J. Corp. L. 46, 909.

Kallel, A., N. B. D. Mouelhi, W. Chaouali, and N. P. Danks (2023). Hey chatbot, why do you treat me like other people? the role of uniqueness neglect in human-chatbot interactions. Journal of Strategic Marketing, 1–17.

Kubicek, J. (2018). Complications of Cryptocurrency: Financial and Cybersecurity Risk in the Age of Bitcoin. Ph. D. thesis, Utica College.

Kwapień, J., M. Wątorek, and S. Drożdż (2021). Cryptocurrency market consolidation in 2020-2021. Entropy 23(12).

Kyle, A. S. and A. A. Obizhaeva (2016). Market microstructure invariance: Empirical hypotheses. Econometrica 84(4), 1345 – 1404.

Lin, M.-B., B. Wang, F. Bocart, C. Hafner, and W. Härdle (2022). Dai digital art index: A robust price index for heterogeneous digital assets. SSRN. Available at SSRN: https://ssrn.com/abstract=4279412.

Long, H., E. Demir, B. Będowska-Sójka, A. Zaremba, and S. J. H. Shahzad (2022). Is geopolitical risk priced in the cross-section of cryptocurrency returns? Finance Research Letters 49, 103131.

Machado, M. R. and S. Karray (2022). Assessing credit risk of commercial customers using hybrid machine learning algorithms. Expert Systems with Applications 200, 116889.

Maghyereh, A. and H. Abdoh (2020). Tail dependence between bitcoin and financial assets: Evidence from a quantile cross-spectral approach. International Review of Financial Analysis 71, 101545.

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. Law, innovation and technology 9(2), 269–300.

Ogbonna, O. E., I. A. Mobosi, and O. W. Ugwuoke (2020). Economic growth in an oil-dominant economy of nigeria: The role of financial system development. Cogent Economics & Finance.

Pele, D. T., N. Wesselhöfft, W. K. Härdle, M. Kolossiatis, and Y. G. Yatracos (2021). Are cryptos becoming alternative assets? The European Journal of Finance, 1–42.

Ren, B. and B. Lucey (2022). A clean, green haven?—examining the relationship between clean energy, clean and dirty cryptocurrencies. Energy Economics 109, 105951.

Roohparvar, R. (2022). The Cybersecurity Risks of Cryptocurrency. https://www.infoguardsecurity.com/the-cybersecurity-risks-of-cryptocurrency/). [Online; accessed 09-May-2023].

Senyo, P. and E. L. Osabutey (2020). Unearthing antecedents to financial inclusion through fintech innovations. Technovation 98, 102155.

Senyo, P. K., D. Gozman, S. Karanasios, N. Dacre, and M. Baba (2022, July). Moving away from trading on the margins: Economic empowerment of informal businesses through fintech. Information Systems Journal. Special Issue Paper.

Tavana, M., A.-R. Abtahi, D. Di Caprio, and M. Poortarigh (2018). An artificial neural network and bayesian network model for liquidity risk assessment in banking. 275, 2525–2554. Publisher: Elsevier.

Teng, H.-W., M.-H. Kang, and L.-C. B. Lee, I-Han (2023). Bridging accuracy and interpretability: A rescaled cluster-then-predict approach for enhanced credit scoring. Available at SSRN 4355268.

Trevisi, C., R. M. Visconti, and A. Cesaretti (2022). Non-fungible tokens (nft): business models, legal aspects, and market valuation. Media Laws, June 21, 2022.

Trimborn, S. and W. K. Härdle (2018). Crix an index for cryptocurrencies. Journal of Empirical Finance 49, 107–122.

Umar, Z., A. Abrar, A. Zaremba, T. Teplova, and X. V. Vo (2022). Network connectedness of environmental attention—green and dirty assets. Finance Research Letters 50, 103209.

University of Cambridge (2023). Cambridge bitcoin electricity consumption index. https://ccaf.io/cbeci/index. Accessed on 9-May-2023.

Urom, C., G. Ndubuisi, and K. Guesmi (2022). Dynamic dependence and predictability between volume and return of non-fungible tokens (nfts): The roles of market factors and geopolitical risks. Finance Research Letters 50, 103188.

Vayanos, D. and J. Wang (2012). Theories of liquidity. Foundations and Trends® in Finance 6(4), 221–317.

Vayanos, D. and J. Wang (2013). Chapter 19 - market liquidity—theory and empirical evidence *. Volume 2 of Handbook of the Economics of Finance, pp. 1289–1361. Elsevier.

Wang, Y., B. Lucey, S. Vigne, and L. Yarovaya (2022). "An index of cryptocurrency environmental attention (ICEA)". China Finance Review International 12(3), 378–414.

Wilson, K. B., A. Karg, and H. Ghaderi (2022). Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity. Business Horizons 65(5), 657–670.

Woitschig, P., G. S. Uddin, T. Xie, and W. K. Härdle (2023). The energy consumption of the ethereum-ecosystem. Available at SSRN 4526732.

Yousaf, I. and L. Yarovaya (2022). Herding behavior in conventional cryptocurrency market, non-fungible tokens, and defi assets. Finance Research Letters 50, 103299.

Zhang, H.-G., C.-W. Su, Y. Song, S. Qiu, R. Xiao, and F. Su (2017). Calculating value-at-risk for high-dimensional time series using a nonlinear random mapping model. Economic Modelling 67, 355–367.

Zihan, Y., L. Yihan, and T. Yinwen (2023). The development and impact of fintech in the digital economy. Economics 12(1), 24–31.

Șcheau, M. C., S. L. Crăciunescu, I. Brici, and M. V. Achim (2020). A cryptocurrency spectrum short analysis. Journal of Risk and Financial Management 13(8), 184.