



REGULATION OF DEFI IN CANADA: CHALLENGES AND PROSPECTS

by

Gulnoza Abdurakhmonova

This thesis is submitted in partial fulfillment of
the requirements
for the degree of Master of Laws at
Dalhousie University,
Halifax, Nova Scotia
August 2024

Dalhousie University is located in Mi'kma'ki, the ancestral
and unceded territory of the Mi'kmaq. We are all Treaty
people.

© Copyright by Gulnoza Abdurakhmonova, 2024

Dedication

This thesis is dedicated to my loving family, whose unwavering support and encouragement have been my greatest source of strength throughout this journey. To my husband, thank you for your endless patience, love, and understanding. To our parents, your prayers and belief in me have been instrumental in reaching this milestone.

A special thank you to my supervisor, Professor Michael Deturbide, for your exceptional mentorship and invaluable guidance. Your insights and encouragement have made this work possible. I would also like to express my deepest gratitude to Colin Jackson for his invaluable suggestions and critical comments which greatly enhanced the quality of this thesis.

Thank you all for being a part of this journey.

Table of Contents

| | |
|---|-----|
| List of Abbreviations Used | iv |
| Abstract | vii |
| Chapter I: Introduction. | 1 |
| Chapter II: Scope of DeFi. | 7 |
| Chapter III: The Evolution of Finance: Unveiling the Distinctions and Impact of DeFi, Fintech, and Cryptocurrencies | 18 |
| Chapter IV: Regulatory Challenges and Concerns | 32 |
| Chapter V: Fintech and Financial Regulations – Can DeFi be regulated? | 41 |
| Chapter VI: Overview of Canadian Law | 48 |
| Chapter VII: Understanding the Regulatory Hurdles for DeFi: Securities Law in a Decentralized World. | 63 |
| Chapter VIII: Consumer protection considerations: disclosure, transparency, privacy and cybersecurity. | 94 |
| Chapter IX: Tax Treatment of Virtual Assets | 104 |
| Chapter X: Environmental considerations of token mining and issuance. | 109 |
| Chapter XI: Conclusion. | 116 |
| Reference list | 120 |

List of Abbreviations Used

| Abbreviation | Full Form |
|--------------|---|
| AML | Anti-money laundering |
| AML/CFT | Anti-money laundering and countering the financing of terrorism |
| CBDC | Central Bank Digital Currency |
| CFT | Combating the financing of terrorism |
| CSA | Canadian Securities Administrators |
| CTP | Crypto-Asset Trading Platform |
| DAO | Decentralised Autonomous Organisations |
| DApps | Decentralized Apps |
| DeFi | Decentralised Financing |
| DEX | Decentralised Exchanges |
| DLT | Digital Ledger Technologies |
| DLT | Distributed Ledger Technology |
| ESG | Environmental, social, and governance |
| GST/HST | Goods and services/harmonized sales tax |

| Abbreviation | Full Form |
|---------------------|---|
| AML | Anti-money laundering |
| AML/CFT | Anti-money laundering and countering the financing of terrorism |
| CBDC | Central Bank Digital Currency |
| CFT | Combating the financing of terrorism |
| CSA | Canadian Securities Administrators |
| CTP | Crypto-Asset Trading Platform |
| DAO | Decentralised Autonomous Organisations |
| ICO | Initial Coin Offering |
| ITO | Initial token offerings |
| KYC | Know your customer |
| MSB | Money Services Business |
| NFT | Non fungible tokens |
| PoA | Proof of Authority |
| PoS | Proof of Stake |

| Abbreviation | Full Form |
|---------------------|---|
| AML | Anti-money laundering |
| AML/CFT | Anti-money laundering and countering the financing of terrorism |
| CBDC | Central Bank Digital Currency |
| CFT | Combating the financing of terrorism |
| CSA | Canadian Securities Administrators |
| CTP | Crypto-Asset Trading Platform |
| DAO | Decentralised Autonomous Organisations |
| PoW | Proof of Work |
| PRU | Pre-registration undertaking |
| VRCA | Value-Referenced Crypto Assets |

Abstract

The emergence of Decentralized Finance (DeFi) has brought about transformative changes in the financial landscape, challenging traditional regulatory frameworks. This thesis provides a comprehensive exploration of the regulatory complexities and challenges surrounding DeFi in Canada, highlighting its growth and significance. It begins by exploring the evolution and disruptive potential of DeFi, particularly its capacity to reshape traditional financial paradigms. A historical context of financial regulation highlights its limitations in managing DeFi's decentralized nature. The study also outlines the rapid growth of DeFi and explains the foundational technologies of Blockchain and Distributed Ledger Technology (DLT), which drive DeFi innovations. Key components of DeFi, such as Bitcoin, cryptocurrencies, and Smart Contracts, are examined for their significance and regulatory complexities. The interplay between Smart Contracts and existing regulatory frameworks reveals the challenges faced by regulators. Additionally, the study scrutinizes the current Fintech and financial regulations, illustrating their inadequacy in addressing the decentralized aspects of DeFi. A detailed overview of Canadian law assesses the existing regulatory framework's relevance to DeFi, including tax treatment of virtual assets and regulations for Stablecoins and Decentralized Exchanges. The thesis also explores the prevalence of DeFi-related fraud and suggests strategies to protect investors. Consumer protection measures, such as disclosure, transparency, privacy, and cybersecurity, are discussed to enhance trust and mitigate risks. Environmental concerns related to token mining and issuance are also considered, with an emphasis on sustainability. The thesis ultimately provides insights into the regulatory challenges of DeFi in Canada, offering recommendations for policymakers, regulators, and market participants navigating this rapidly evolving space.

Keywords: Blockchain, DeFi, Sustainability, DLTs, Cryptocurrencies, Smart Contracts, Tax Treatment, Stablecoins, Decentralized Exchanges (DEX), Fraud Prevention, Consumer Protection, Cybersecurity, Sustainability, Market Integrity.

Chapter I: Introduction.

We stand at a pivotal moment of the financial landscape. Once, our economic exchanges relied on direct peer-to-peer transactions, known as bartering, but this method proved outdated and inefficient. It required a perfect match of supply and demand between individuals. To solve this, money emerged as a medium of exchange and store of value. Early money was decentralized, with people accepting various items like stones or shells in trade¹. Over time, this evolved into distinct currencies, each with tangible value. In the contemporary landscape, we navigate a realm dominated by non-collateralized (fiat) currency, meticulously regulated by central banks. While the form of money has undergone transformations over time, the foundational structure of financial institutions has remained remarkably unaltered.² Nevertheless, an unprecedented transformation looms, signifying a historic disruption of our existing financial framework. The rise of DeFi represents a significant shift, aiming to combine open-source financial tools into advanced products using blockchain technology. DeFi seeks to reduce friction and enhance value for users, driven by the idea that service costs are consistent regardless of asset value. This has led to the belief that DeFi could eventually replace key parts of centralized financial systems. This transformative force embodies a technology of inclusion, enabling anyone to access and benefit from DeFi innovations through a flat fee. Unlike traditional banking systems, which often impose varying fees and barriers based on factors like account balance or transaction size, DeFi operates on principles of equality and accessibility. In DeFi, every user, regardless of their asset value or financial status, is treated equally and incurs the same costs for accessing services. This democratization of financial services stands in stark contrast to the hierarchical and exclusionary nature of traditional banking, where fees, minimum balances, and other restrictions often disproportionately affect those with lower incomes or fewer assets. Additionally, DeFi operates

¹ Henri Arslanian, "The History of Money" in *The Book of Crypto* (Cham: Palgrave Macmillan, 2022) 1 at 43, online: https://doi.org/10.1007/978-3-030-97951-5_22.

² Ibid

without the need for intermediaries like banks, allowing for greater transparency, efficiency, and autonomy in financial transactions.

DeFi fundamentally operates as a competitive marketplace, housing decentralized financial applications functioning as diverse financial "primitives," encompassing exchanges, savings, lending, and tokenization. The synergistic effects derived from combining and recombining DeFi products position these applications to steadily accrue market share from the traditional financial ecosystem. Regulating DeFi is imperative to ensure the safeguarding of investors and the integrity of the market. A functional regulatory approach is essential to achieve outcomes in line with investor protection and market integrity goals, mirroring or aligning with the standards upheld in traditional financial markets.³

While the decentralized nature of DeFi offers numerous advantages, such as increased accessibility and autonomy, it also introduces significant risks that necessitate careful consideration. Without centralized oversight, DeFi platforms can become breeding grounds for fraudulent activities. Investors may fall victim to Ponzi schemes, phishing scams, or yield farming⁴ projects promising unrealistic returns, only to lose their funds due to malicious actors or vulnerabilities in the system. Implementing a functionally based regulatory framework will enable authorities to address specific aspects of DeFi operations, tailoring regulations to ensure investor security and market stability. Balancing innovation and risk mitigation is essential for DeFi's sustainable growth. A well-designed regulatory approach can protect participants while preserving the advantages of decentralized finance.

In recent years, the financial landscape has witnessed a transformative shift with the emergence of DeFi – a groundbreaking ecosystem that leverages blockchain technology to recreate

³ IOSCO - Policy Recommendations for Decentralized Finance (DeFi) Consultation Report CR/04/2023 September 2023 - <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf>

⁴ Yield farming, a widely adopted practice within the realm of decentralized finance (DeFi), stands as a prominent method for managing assets. This practice encompasses actions such as providing, borrowing, or staking cryptocurrency assets to garner earnings through various means, including transaction fees, interest accrual, or rewards for participation across diverse DeFi platforms. (Jiahua Xu & Yebo Feng, "Reap the Harvest on Blockchain: A Survey of Yield Farming Protocols," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 858-869 (March 2023) doi: 10.1109/TNSM.2022.3222815.)

traditional financial services in a decentralized and permissionless manner. Canada, like many other countries, has not been immune to the disruptive force of DeFi. As the DeFi space gains momentum and captures the attention of market participants, policymakers in Canada find themselves at a critical juncture, tasked with the challenge of defining a regulatory framework that balances innovation with investor protection, financial stability, and compliance.

The rise of DeFi in Canada is marked by the proliferation of blockchain-based platforms offering an array of financial services such as lending, borrowing, trading, and yield farming, all without the need for traditional intermediaries. Smart contracts, powered by blockchain networks like Ethereum, form the backbone of these decentralized applications (“DApps”), enabling users to transact seamlessly and securely without reliance on centralized entities. While traditional legal contracts themselves may not inherently rely on centralized entities, their enforcement and the broader financial systems they operate within often do, particularly when involving regulated markets or securities. In contrast, smart contracts are self-executing agreements with the terms directly written into code, functioning independently of such centralized infrastructures and providing a new paradigm for trustless transactions.

The decentralized nature of DeFi promotes financial inclusion but poses regulatory challenges for Canadian authorities. The lack of intermediaries and the global scope of blockchain networks complicate jurisdiction, accountability, and enforcement. The rapid innovation in DeFi further strains traditional regulatory frameworks, making it difficult to keep up. As DeFi grows in capital and user engagement, concerns about market integrity, consumer protection, and anti-money laundering have led Canadian regulators to reassess their approach. Balancing innovation with investor and financial system protection is now a key focus, prompting a review of existing regulations and potential adaptations. This thesis delves into the multifaceted landscape of DeFi regulation in Canada, aiming to provide a comprehensive analysis of the challenges and opportunities that arise at the intersection of decentralized finance and the Canadian regulatory environment. Through an exploration of current regulatory initiatives, industry trends, and the

global context, this research aims to contribute to the ongoing dialogue surrounding the formulation of a robust and adaptive regulatory framework for DeFi in Canada. In this way, the thesis provides a structured exploration of DeFi, moving from conceptual definitions to specific regulatory concerns, and ultimately offering a coherent narrative on the regulation of DeFi within the Canadian legal system.

To further guide this research, the following key questions have been developed to address the core challenges and prospects of DeFi regulation in Canada. How does DeFi differ from traditional financial technologies, and what unique regulatory challenges does it present? To what extent can DeFi be integrated into existing regulatory frameworks, particularly in the context of securities law and financial regulations? What are the implications of DeFi for Canadian law, including considerations of consumer protection, privacy, and cybersecurity? Additionally, how should the tax treatment of virtual assets and the environmental impact of token mining be approached within the Canadian regulatory landscape? These questions will form the foundation of this thesis, guiding the exploration of whether and how DeFi can be effectively regulated while fostering innovation and safeguarding key interests.

The thesis begins with the introduction of the scope of DeFi by outlining its core concepts, principles, and operations. This section sets the foundation for understanding how DeFi distinguishes itself from traditional finance and other related technologies. Moving into the next section, I explore the evolution of finance, examining the distinctions between DeFi, Fintech, and cryptocurrencies. Here, I compare how these three innovations impact the financial industry and explain why DeFi represents a significant shift within the broader landscape of financial technology.

In the section IV, I turn to the various regulatory challenges and concerns raised by DeFi. This section highlights the complexities DeFi presents to regulators, including issues related to its decentralized nature, anonymity, and jurisdictional ambiguity, all of which make traditional regulatory approaches difficult to apply.

Section V then poses a critical question: Can DeFi be regulated? By examining how Fintech has been regulated in comparison, this section delves into whether DeFi, with its unique characteristics, can be integrated into existing regulatory frameworks. This exploration is a prelude to later discussions of regulatory adaptations or new frameworks that may be necessary. Sections V through VIII collectively address the central regulatory issues raised by DeFi, especially within Canada. These sections outline the primary challenges in trying to fit decentralized technologies into traditional financial regulatory frameworks, touching on key themes such as jurisdiction, transparency, privacy, and consumer protection, providing an overview of the current Canadian financial regulatory landscape and explore how existing laws may (or may not) accommodate DeFi, laying the groundwork for the more detailed regulatory analyses that follow. These sections form the core of the thesis's discussion on how to regulate DeFi in a coherent and practical way.

Section VII delves into the regulatory hurdles that DeFi faces, particularly through the lens of Canadian securities law. It explores how decentralized technologies and platforms challenge traditional securities regulations. In this section, I further discuss the regulatory challenges and gaps in the oversight of stablecoins, focusing on securities-related risks, macroprudential concerns, and the need for banking-like safeguards. Additionally, I analyze the regulation of decentralized exchanges (DEXs) and virtual asset service providers (VASPs), both of which play a crucial role in the DeFi ecosystem. Moreover, the section addresses the growing issue of DeFi fraud and the need to safeguard investors within this rapidly evolving landscape. I highlight the importance of legal protections and frameworks for fighting DeFi fraud, outlining key measures that could enhance investor protection and prevent fraudulent activities in the decentralized financial space.

In the section on Tax treatment of Virtual Assets, I examine the tax implications of DeFi and other virtual assets. This section explores the current approaches to taxing virtual assets and raises questions about whether these assets should be treated differently from more traditional financial products under tax law. In the last section of my thesis, I will briefly consider the

environmental impacts of DeFi, particularly the energy consumption associated with token mining and issuance. This section highlights the growing concern over the environmental sustainability of blockchain technologies and their implications for regulatory oversight.

Finally, the conclusion part provides some final thoughts on how Canadian law might evolve to address the unique challenges posed by DeFi and synthesizes the findings from the previous sections. The conclusion also identifies areas for future research and discusses the potential for international cooperation in developing a more comprehensive regulatory framework for decentralized finance.

Chapter II: Scope of DeFi.

DeFi refers to a novel financial ecosystem built on blockchain technology that seeks to recreate and enhance traditional financial services in a decentralized manner. Unlike traditional financial systems that rely on centralized authorities such as banks and intermediaries, DeFi leverages smart contracts, DApps, and blockchain protocols to facilitate and automate various financial transactions and services. The scope of DeFi encompasses a wide array of financial activities, including but not limited to lending, borrowing, trading, insurance, and asset management. These services are typically provided through decentralized platforms, allowing users to interact directly with smart contracts and conduct financial transactions without the need for intermediaries. This not only reduces the reliance on traditional financial institutions but also aims to enhance financial inclusivity by providing access to financial services to a broader global audience. However, it is worth noting that the lack of intermediaries in DeFi means there are no traditional banks or brokers to oversee transactions, provide consumer protection, or ensure regulatory compliance. This absence can lead to increased risks of fraud, security breaches, and loss of funds due to user error or vulnerabilities in smart contracts. Moreover, without intermediaries, there's no recourse for users if something goes wrong, which can deter individuals who rely on the safety nets provided by conventional financial institutions.

Key components of DeFi include:

- Smart Contracts: DeFi relies heavily on smart contracts, which are self-executing contracts with the terms of the agreement directly written into code.⁵ These contracts automate and enforce the execution of financial transactions without the need for intermediaries.
- Decentralized Exchanges (DEXs): DEXs enable users to trade various cryptocurrencies and tokens directly without relying on centralized exchanges⁶. This shift towards decentralization aligns with blockchain's core principle of transparency, where transactions

⁵ Chris Brummer, "Disclosure, DApps and DeFi" (2022) 5:2 Stanford Journal of Blockchain Law & Policy 137-174, available at <https://assets.pubpub.org/efeeza8o/01656289809141.pdf>.

⁶ Ibid

and data are openly accessible and resistant to alteration. Such transparency surpasses conventional industry structures. Blockchain technology facilitates this transparency by enabling anyone to scrutinize the underlying code, including smart contracts, which operate on open-source blockchain software. Consequently, transaction outcomes remain continuously visible on the blockchain ledger, albeit requiring a certain level of expertise for accurate interpretation. Through DEXs, this heightened transparency fosters enhanced security, transparency, and control over one's assets⁷.

- Lending and Borrowing Platforms: DeFi platforms enable users to lend or borrow digital assets directly through smart contracts, offering an alternative to traditional institutions by potentially streamlining the process and reducing reliance on intermediaries.
- Stablecoins: DeFi often utilizes stablecoins, which are cryptocurrencies pegged to the value of traditional fiat currencies. These stablecoins provide a more stable unit of account and medium of exchange within the DeFi ecosystem.
- Decentralized Autonomous Organizations (DAOs): DAOs are organizations governed by smart contracts and consensus mechanisms, enabling decentralized decision-making among stakeholders.

Smart contracts have the potential to integrate and engage with each other within a decentralized and distributed framework. Once deployed by their developers, these contracts operate independently, devoid of human intervention, and adhere to the rules and mechanisms embedded in their programming⁸. This concept extends to the formation of DAOs, which possess the capability to establish new smart contracts with other participants in the market. This dynamic gives rise to a sophisticated and evolving ecosystem where various agents interact through pre-

⁷ Ibid

⁸ Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (March 10, 2015), online: SSRN <https://ssrn.com/abstract=2580664> or <http://dx.doi.org/10.2139/ssrn.2580664> p. 15;

established, hardcoded, and self-enforcing rules⁹. Importantly, DAOs lack singular ownership or control by any individual or entity, yet they maintain the ability to interact within the market¹⁰.

A noteworthy DAO to date emerged through the utilization of smart contracts documented and executed on the Ethereum network. This particular DAO represents a novel concept—a venture capital firm devoid of human intervention, where investors collectively determine outcomes through smart contracts. The absence of leaders or authorities is a defining feature, as the decision-making process is guided solely by rules encoded by humans and executed through computer protocols¹¹. This DAO successfully garnered an impressive \$150 million, but unfortunately, a malicious node redirected \$50 million to a private Internet address, leading to the abandonment of the project. Despite this setback, there is a possibility of similar ventures emerging in the future. On the other hand, it remains uncertain whether the financial industry will show interest in fully autonomous, self-referential entities. While profit-driven organizations often seek to maintain legal and economic ties with their operations to ensure control and compliance, there is also a growing trend to reduce costs and increase profitability through automation and minimizing reliance on human workers. The concept of entirely autonomous, self-executing software raises questions about the extent to which smart contracts on a blockchain network can operate independently from human involvement, varying in autonomy on different scales. These contracts can exchange input in the form of reference data and trigger events, potentially spanning across various blockchain networks. As smart contracts become more interconnected and operate with less direct human oversight, the governance of these autonomous systems presents unique challenges, distinct from the governance of human behavior. While human conduct can be unpredictable, the complexity and lack of transparency in interconnected smart contracts can also make regulation difficult¹².

⁹ Ibid p. 17.

¹⁰ Ibid p. 54

¹¹ J.I. Wong and I. Karr, ‘Everything you need to know about the Ethereum “Hard Fork”’, Quartz (18 July 2016), <http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/>, visited 30 Nov. 2016.

¹² Philipp Paech, "The Governance of Blockchain Financial Networks" (2017) 80(6) *Modern Law Review* 1073–1110, LSE Legal Studies Working Paper No. 16/2017, online:

While DeFi offers numerous benefits, such as increased accessibility, transparency, and efficiency, it also poses certain challenges and risks. Regulatory uncertainty, smart contract vulnerabilities, and the potential for fraudulent activities are among the concerns that need to be addressed to ensure the sustainable growth of the DeFi space. In legal terms, the regulatory status of DeFi varies globally, and jurisdictions are actively working to establish frameworks that govern these decentralized financial activities. As the industry evolves, it is crucial for regulators to strike a balance between fostering innovation and ensuring consumer protection, market integrity, and compliance with existing legal frameworks. In the subsequent chapters, I will delve into the regulatory hurdles confronting both the DeFi sector and regulatory bodies.

- Blockchain and DLT explained.

This section of the chapter will explore the fundamental concepts of Distributed Ledger Technology (DLT), Blockchain, and Smart Contracts, focusing on their application and significance within the decentralized finance (DeFi) ecosystem. These technologies serve as the backbone of DeFi, enabling the creation of secure, transparent, and decentralized financial systems. Understanding their mechanisms and implications is essential to grasp the transformative potential they hold for the financial industry. The discussion is vital to lay the groundwork for the subsequent analysis of DeFi, providing a comprehensive understanding of the technological underpinnings that drive this emerging field.

The blockchain constitutes a form of distributed ledger technology (“DLT”), operating as a decentralized database or ledger. In this system, data is distributed across multiple computers or nodes, eliminating the need for an intermediary to validate digital asset transfers. Within a DLT framework, nodes represent the devices running DLT software responsible for collectively upkeeping the database records. This configuration facilitates interconnectivity among nodes, enabling the direct sharing and validation of information. At its most extensive, this structure empowers any entity possessing a node to engage in shared database management responsibilities

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3082805_code1690659.pdf?abstractid=2875487&mirid=1&type=2

directly with others in a peer-to-peer manner¹³. Moreover, experts argue that DLT encompasses four key features: ‘shared record keeping, multi-party consensus, independent validation, tamper evidence and resistance’.¹⁴ Hence, the distributed ledger of transactions serves as the sole authoritative record that a substantial number of participants can trust, yet none of them can individually dominate. Consequently, the DLT platform supporting virtual currencies is distinguished by decentralization, immutability, and a trustless system (without any intermediaries).¹⁵

The utilization of blockchain technologies seems to be challenging the traditional roles of central actors and processes crucial for global governance. This shift may not always align with normative desirability¹⁶. Blockchains are being utilized to enhance and facilitate various governance functions. The innovation and expansiveness of the increasing use of blockchain technology have generated optimistic pledges and apprehensive concerns about its applications not only to Bitcoin but also in broader contexts¹⁷. Some scholars argue that enabling transactions to circumvent banks and other financial institutions, which typically oversee and provide states with income data, often eludes conventional global tax governance mechanisms, potentially leading to the emergence of "super tax havens."¹⁸ While cryptocurrencies operate within a trustless system that maintains perfect records through blockchain technology, they are not immune to losses or theft. These incidents can occur due to various factors, such as hacking, loss of private keys, or fraudulent schemes. Unlike traditional financial systems, which often provide recourse through centralized authorities like banks or regulatory bodies, users of alternative coins

¹³ D. Mills, K. Wang, B. Malone et al, "Distributed Ledger Technology in Payments, Clearing, and Settlement," Federal Reserve Board Finance and Economics Discussion Series, no 2016-095, December 2016, at 17, www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

¹⁴ Final report of the Expert Group on Regulatory Obstacles to Financial Innovation: 30 recommendations on regulation, innovation, and finance, Final Report to the European Commission, European Commission, Brussels, Belgium, December 13, 2019, https://finance.ec.europa.eu/system/files/2019-12/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf.

¹⁵ Gabriella Gimigliano, "Payment Tokens and the Path Towards MiCA" (2021) 8:1 Ital LJ 381, online: <https://usiena-air.unisi.it/retrieve/1c80bed0-a603-494c-818b-a63c2b4dfed8/gimigliano%20TILJ.pdf>

¹⁶ Malcolm Campbell-Verduyn, ed, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, 1st ed, RIPE Series in Global Political Economy (London: Routledge, 2017), online: <https://doi.org/10.4324/9781315211909>, P. 10

¹⁷ Ibid

¹⁸ Omri Marian, "Are Cryptocurrencies Super Tax Havens?" *Michigan Law Review* 112, no. 1 (2013): at 42–3.

("altcoins")—which are cryptocurrencies other than Bitcoin—often have no such protection. This lack of recourse in the event of a loss or theft has been identified by business ethicists as inequitable, as it leaves users vulnerable without any means to recover their assets.¹⁹

In the context of distributed ledgers utilized in blockchain networks, each party responsible for managing and possessing an asset always possesses an updated identical copy of the record. This record is meticulously designed to prevent discrepancies among the various copies²⁰. Moreover, blockchain technology enables increased data depth, allowing records to accommodate more intricate information compared to conventional accounts²¹. For example, a traditional securities account with a broker solely records ownership details of securities, lacking additional specifics. In contrast, in a prospective blockchain-based scenario, information pertaining to ownership of a specific share could encompass details about the involved service providers, the existence of any encumbrances on the share, and the beneficiaries of such encumbrances. While it's true that a securities intermediary could also record such information if requested, a blockchain system offers a more streamlined and efficient approach, particularly when dealing with jurisdictional boundaries. For instance, in Canada, the existence of 10 different provincial personal property registries to record encumbrances on shares can be quite inefficient. However, the adoption of blockchain for this purpose also raises unresolved questions about how disputes would be managed. For example, it remains unclear how disputes would be resolved regarding the existence or discharge of an encumbrance, or whether a creditor has the right to seize a share given as collateral in the event of a debtor's default. While blockchain could provide a more efficient means of recording and managing these details, the legal and procedural frameworks for resolving such disputes in a decentralized environment are still in development.

- **Decoding the Significance: Smart Contracts**

¹⁹ C. Dierksmeier & P. Steele, "Cryptocurrencies and Business Ethics," *Journal of Business Ethics* (2016) 1–14, <https://doi.org/10.1007/s10551-016-3298-0>.

²⁰ Nakamoto (2008) See note 36

²¹ Pietro Ortolani, "Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin," *Oxford Journal of Legal Studies* 36, no. 3 (Autumn 2016): 608, Oxford University Press.

A smart contract is a self-executing contract with the terms of the agreement between the parties directly written into code. These ingenious digital agreements are the backbone of DeFi and its regulatory landscape. It may be considered as a digital version of a traditional contract, but instead of relying on human interpretation and enforcement, the terms are automatically executed by a computer program. In the context of DeFi, these contracts facilitate and automate various financial transactions, such as lending, borrowing, trading, and investment activities, without the need for traditional intermediaries like banks.

Initially, the term denoted arrangements with unstoppable automatic execution. In practical usage, it frequently encompasses processes with automated execution, acknowledging that certain stages may involve human input and oversight. There remains ambiguity regarding whether a smart contract merely serves as a computerized transaction protocol executing contract terms, or if the smart contract itself binds the agreement between parties.²² In general, smart contracts are commonly seen as effective means to automate certain terms and responsibilities outlined in a legal agreement. Advancing technology places emphasis on the development of smart legal contracts, which tend to obscure the line between conditions specified in code and those laid out in traditional legal contracts²³.

Although smart contracts existed as an independent concept before the advent of blockchain, their optimal functionality is realized when implemented on blockchain or distributed ledger technology (DLT) networks.²⁴ This is due to the assurance of execution provided by these platforms. Because of the authentication and security measures outlined earlier, these mechanisms are reliable for enforcing legal, business, and regulatory rules. The dependable automation of legal contract execution through smart contracts, coupled with the unchangeable nature of transactions

²² Don Tapscott & Alex Tapscott, *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (May 2016) at 72, 83, 101, 127. (in the source: Tapscott, Don; Tapscott, Alex (May 2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. pp. 72, 83, 101, 127)

²³ Philipp Paech (2017), see note 12.

²⁴ T. Butler et al, "Smart Contracts and Distributed Ledger Technologies in Financial Services: Keeping Lawyers in the Loop" (2017) 36(9) *Banking & Financial Services Policy Report* 1-11.

on a blockchain, makes this blend genuinely groundbreaking and disruptive technology. It facilitates the adoption of novel business models and the automation of established ones.

Zero-knowledge proof, also referred to as a zero-knowledge protocol, is poised to enhance the utility of blockchain and DLT, including applications such as smart contracts. This cryptographic method allows one party (the prover) to demonstrate to another party (the verifier) that they possess knowledge of a value x without disclosing any details about x itself. The fundamental concept behind zero-knowledge proofs lies in the ability to validate possession of information or knowledge without divulging the information. This has profound implications for areas such as identity management, authentication, and various cryptographic challenges, particularly within the financial industry. In finance, smart contracts can be effectively employed in various contexts²⁵:

- **Loans and Financing:** Validating transactions, confirming the legitimacy of counterparties, and conducting routine account administration.
- **Mortgages:** Providing a unified platform for the coordination of activities involving lawyers, realtors/estate agents, appraisers, bankers, mortgage brokers, engineers, home buyers, and sellers. This includes validating transactions, verifying counterparties, and facilitating settlements.
- **OTC (Over the Counter) Trading:** Handling transactions of currencies (including cryptocurrencies), commodities, and securities.
- **Derivative Trading:** Matching traders, validating transactions, confirming the legitimacy of counterparties, holding counterparty funds, and settling contracts involving crypto assets like futures contracts, forward contracts, options, swaps, and warrants.
- **Derivatives Markets:** Potentially giving rise to both centralized and decentralized exchanges.

²⁵ Expert Group on Regulatory Obstacles to Financial Innovation (2019), see note 14

- **Insurance Policies:** Streamlining claims management through responsive and transparent processes, employing “know your client” and accurate risk assessment, reducing administration and underwriting costs, ensuring accurate pricing, enabling automated claims submission and processing, enhancing claims assessment and costing, detecting fraud, and facilitating automatic payments. This involves consolidating all agents and parties onto a single platform for increased transparency and integrity.
- **Business-to-customer transactions:** Recording transactions or exchanges involving digital assets.
- **Business-to-business transactions:** Implementing complex payments for asset/payment transactions.
- **Regulatory Reporting:** Leveraging the combination of smart contracts and blockchain for more efficient and transparent automation of regulatory reporting on financial compliance and risk²⁶. This system benefits financial institutions, regulators, and auditors by ensuring transparency, reliability, and efficiency in reporting processes.

In contrast to traditional contracts, where parties can opt to fulfill their obligations or not, smart contracts are immutable. Once the parties agree to be bound by a specific clause, the code of the smart contract irrevocably obligates them to adhere to that clause, eliminating the possibility of breach²⁷. Transactions executed through smart contracts are recorded on a blockchain, a tamper-resistant and transparent digital ledger. This system is often described as 'trustless' because it doesn't require participants to trust a central authority; instead, trust is placed in the decentralized network and the underlying technology. The transparency of the blockchain allows participants to independently verify transactions, further reinforcing confidence in the system.

These developments in DeFi underscore three key advantages:

²⁶ Financial Conduct Authority, Bank of England, "Digital Regulatory Reporting: Pilot 1 Phase Report" (13 March 2019), online: <https://www.fca.org.uk/publication/discussion/digital-regulatory-reporting-pilot-phase-1-report.pdf>.

²⁷ Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (March 10, 2015), online: SSRN <https://ssrn.com/abstract=2580664> or <http://dx.doi.org/10.2139/ssrn.2580664> p.26
Aaron Wright & Primavera De Filippi (2015), see note 27. p.26

- Decentralization: DeFi operates on decentralized networks, meaning there is no central authority controlling the financial activities. Smart contracts enable decentralized governance, allowing users to have more control and ownership over their assets and transactions.
- Accessibility: DeFi services powered by smart contracts are often accessible to anyone with an internet connection, providing financial services to individuals who may be excluded from traditional banking systems.
- Programmable Finance: Smart contracts enable programmable finance, allowing developers to create complex financial instruments and protocols. For example, decentralized lending platforms can automatically match borrowers and lenders based on predefined criteria, while automated market makers (AMMs) like Uniswap facilitate instant, trustless trading of assets without intermediaries²⁸. This flexibility fosters innovation in developing new financial products and services, such as decentralized insurance, yield farming strategies, and synthetic assets.

The challenge of DeFi regulation lies in adapting traditional legal frameworks to this new and rapidly evolving digital landscape. Regulators need to consider how existing laws apply to smart contracts and decentralized systems. Balancing the benefits of innovation with the need for consumer protection and market integrity is crucial. As the legal landscape evolves, finding ways to regulate DeFi without stifling its innovative potential becomes a key focus for legal scholars and lawmakers. Smart contracts, operating on blockchain technology, also pose a challenge to lawyers' traditional role in interpreting ambiguous contract language as they automatically validate and execute pre-encoded contractual terms²⁹. Legal and regulatory language must be accessible to

²⁸ S S, AR Saxena, YR Saxena, MSM Sana, S Verma & S Roy, "Decentralized Finance and Cross-Chain Interoperable Automated Market Maker - Using BlockChain" (2024) in 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, pp 1-9, DOI: 10.1109/ic-ETITE58242.2024.10493513.

²⁹ Quinn DuPont and Bill Maurer, "Ledgers and Law in the Blockchain" (June 23, 2015), UC Irvine, online: <https://escholarship.org/uc/item/6k65w4h3>.

both humans and machines to enhance transparency and efficiency³⁰. This necessitates crafting language that facilitates understanding by all stakeholders, thereby streamlining reporting and compliance processes. Standardization efforts are also crucial, encompassing both legal terminology and digital categorization, particularly concerning smart contracts. Establishing clear definitions within existing legal frameworks is essential to ensure appropriate regulation and foster a uniform understanding across the financial landscape. Consumer protection is paramount, requiring regulations that prioritize transparency in smart contract terms and processes, along with mechanisms to address disputes and safeguard users from potential risks.

³⁰ Expert Group on Regulatory Obstacles to Financial Innovation (2019), see note 14

Chapter III: The Evolution of Finance: Unveiling the Distinctions and Impact of DeFi, Fintech, and Cryptocurrencies

The following discourse seeks to explore the transformative journey of the financial industry, focusing on the evolution from traditional systems to the rise of decentralized finance (DeFi), fintech innovations, and cryptocurrencies. By unraveling the distinctions between DeFi and fintech, it aims to highlight how these emerging technologies are reshaping global finance. Additionally, the impact of Bitcoin and other cryptocurrencies is examined, with a focus on their role within this rapidly changing landscape and their implications for the future of financial systems.

In the early stages of market exchanges, transactions were conducted directly between peers, forming a peer-to-peer system. The limitations of this barter system, requiring a precise match of two parties' needs, led to the emergence of an informal credit system in villages, where individuals maintained mental records of reciprocal "gifts." The introduction of coinage occurred later, with the advent of the first modern coins in Lydia around 600 BCE, providing conventional monetary functions such as being a unit of account, a medium of exchange, and a store of value³¹. Noteworthy characteristics of money, including durability, portability, divisibility, uniformity, limited supply, acceptability, and stability, were inherent in these early monetary systems. The inception of bank notes, originating in China, reached Europe in the 13th century. The non-physical transfer of money began in 1871 with the introduction of Western Union. Subsequent innovations included RFID payments (1997) with Mobil Speedpass, chip and pin credit cards (2005), and the introduction of Apple Pay (2014). Importantly, these innovations, while transformative, were underpinned by the existing centralized financial infrastructure. Even though the digitization advancements represented a crucial innovation, they primarily served to support a legacy financial structure. The persistent high costs associated with this legacy system spurred

³¹ Henri Arslanian (2022) 1 at 43, See note 1.

further developments in the form of Fintech, which emerged as a response to the need for more efficient and cost-effective financial solutions.³²

In instances of elevated costs, innovation tends to emerge to exploit inefficiencies, although the presence of influential intermediaries can impede the pace of such innovation. In the early 2000s, a fintech startup³³ proposed an alternative approach, suggesting the establishment of an electronic system to directly match buyers and sellers at agreed-upon prices, eliminating the spread. This system, offered by banks to their customers for a modest fee, aimed to enhance efficiency and reduce unnecessary foreign exchange transaction costs incurred by large corporations dealing with multiple banks. Despite potential concerns about cannibalizing existing profit centers, banks recognized the dissatisfaction among their largest customers due to globalization-induced foreign exchange transaction costs. This decentralized approach sought to address these concerns and streamline foreign exchange transactions through a peer-to-peer network.

An early example of fintech innovation can be traced back to 1979 with the introduction of dark pool stock trading, enabled by the US SEC's Rule 19c3³⁴. This rule allowed large institutions to trade stocks off-exchange, reducing costs compared to traditional exchanges. In more recent years, cost-reducing fintech innovations like PayPal and Zelle have emerged, both of which, despite their advancements, rely on the centralized infrastructure of the existing financial system. This highlights the interconnected relationship between new fintech developments and the traditional financial framework³⁵. The numerous digital currency endeavors that commenced in

³² Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro, *DeFi and the Future of Finance* (April 5, 2021), available at <https://compoundmaven.com/wp-content/uploads/2022/08/DeFi-And-The-Future-Of-Finance-Duke-University-August-2021.pdf>

³³ "Forex goes into future shock," *Euromoney*, October 2001, <https://people.duke.edu/~charvey/Media/2001/EuromoneyOct01.pdf>.

³⁴ Exchange Act Release No. 15769 (April 26, 1979), 44 FR 26688. Rule 19c-3 prevents off-board trading restrictions on securities listed after April 26, 1979, from being applicable.

³⁵ Harvey et al., 2021, p.9, See note 32.

the early 1980s all ended in failure³⁶. However, a pivotal shift occurred with the release of the renowned Satoshi Nakamoto Bitcoin white paper in 2008³⁷. This document introduced a decentralized, peer-to-peer system utilizing the concept of blockchain. While the idea of blockchain originated in 1991 through the work of Haber and Stornetta,³⁸ was initially conceived as a time-stamping system for tracking different document versions. What set Bitcoin apart was the amalgamation of blockchain (for time stamping) with the consensus mechanism called Proof of Work, introduced by Adam Back in 2002³⁹. This technological fusion resulted in an immutable ledger, addressing a fundamental issue with digital assets - the potential for perfect copies and multiple expenditures.

Blockchains, as exemplified by Bitcoin, offer essential features that were previously absent in a singular asset. These features include cryptographic scarcity (Bitcoin is subject to a maximum supply limit of 21 million coins), censorship resistance, and user sovereignty (where only the user can determine fund utilization), along with portability (enabling the transfer of any quantity anywhere for a low flat fee). The convergence of these attributes within a single technology renders cryptocurrency a potent and innovative force. Satoshi Nakamoto characterized it as a "digital coin." This digital currency is comprised of a sequence of digital signatures that can be moved from the sender to the receiver by digitally signing a hash of the preceding transaction and the public key of the subsequent owner, and appending them to the coin's end⁴⁰. In other words, the transfer process involves digitally signing a code that represents the previous transaction, along with the public key of the new owner. These digital signatures are then added to the end of the digital coin, facilitating secure and traceable transactions between parties.

³⁶ Campbell R. Harvey, "The History of Digital Money" (2020), online: https://faculty.fuqua.duke.edu/~charvey/Teaching/697_2020/Public_Presentations_697/History_of_Digital_Money_2020_697.pdf.

³⁷ Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), online: <<https://bitcoin.org/bitcoin.pdf>>

³⁸ S. Haber, W.S. Stornetta, "How to time-stamp a digital document," *Journal of Cryptology* 3, no. 2 (1991): 99-111

³⁹ Hashcash was proposed in 1997 by Adam Back and described more formally in Back's 2002 paper: Adam Back, "Hashcash-A Denial of Service Counter-Measure" (1st August 2002), online: <http://www.hashcash.org/papers/hashcash.pdf>.

⁴⁰ Nakamoto (2008), See note 37

The Bitcoin network operates through autonomous nodes, each managed by a 'miner.' Miners aggregate proposed payments into a new block for the blockchain. This block undergoes a hashing process, wherein the data, along with other information, is repeatedly processed through a cryptographic 'hash' function. The resulting hash is incorporated into the block's header, forming the basis for a challenging mathematical puzzle. Miners engage in competition to solve this puzzle, and the first one to provide the correct solution, validated by the majority of miners through 'proof of work,'⁴¹ is rewarded with newly created bitcoins. Although the mathematical puzzle is intricate, once solved, it is easily verifiable by the network. Nodes accept the block by adding it to the chain, linked to the first Bitcoin block (genesis block) that contains the initial transaction in the Bitcoin network. This structure is designed to ensure the tamper-proof nature of the Bitcoin blockchain. Any attempt to manipulate a transaction by altering a block already stored in the blockchain would result in a different hash, detectable by all as evidence of tampering. The 'coin' encapsulates its entire history, making each payment an integral part of its code⁴².

Understanding the value proposition of Bitcoin is crucial, and it becomes clearer when compared to the value propositions of other financial assets. The US dollar ("USD"), for instance, was historically backed by gold until the abandonment of the gold standard in 1971.⁴³ Unexpected changes in the supply of the USD can influence its price at a given level of demand. The Federal Reserve has the power to adjust the supply through monetary policy, aiming to achieve various financial or political objectives. Inflation poses a threat to the value of the USD, diminishing its ability to serve as a reliable store of value over time. Concerns about runaway inflation, such as Paul Tudor Jones' concept of "The Great Monetary Inflation," may drive investors towards assets resistant to inflation⁴⁴. Gold, with its limited supply, practical utility, and global trustworthiness,

⁴¹ In accordance with Satoshi Nakamoto's whitepaper, "[proof-of-work is essentially one-CPU-one-vote," rather than "one-IP address-one-vote".

⁴² Benjamin Geva, "Cryptocurrencies and the Evolution of Banking, Money and Payments" in Chris Brummer (ed.), *Cryptoassets: Legal, Regulatory and Monetary Perspectives* (Oxford University Press, 2019) at 11-38.

⁴³ Harvey et al. (2021) See note 32.

⁴⁴ Ibid

has historically served as a successful inflation hedge. However, its price volatility limits its hedging effectiveness to extremely long-time horizons.

As highlighted by Stanford economist Susan Athey, digital currencies have the potential to broaden international commerce, promote financial inclusion, and revolutionize various aspects of shopping, saving, and conducting business in ways that may currently be beyond our full comprehension⁴⁵. Cryptocurrencies have the potential to offer considerable advantages by addressing issues related to the absence of social trust and enhancing accessibility to financial services⁴⁶. They may serve as a means to foster development in developing nations by promoting financial inclusion, improving fund traceability, and assisting individuals in breaking free from poverty⁴⁷. Cryptocurrencies have the potential to reduce poverty by providing unbanked and underbanked populations with access to secure, low-cost financial services, thereby enabling greater economic participation and growth. However, this potential is accompanied by challenges that must be carefully considered. Some scholars argue that the majority of what are termed cryptocurrencies lack the fundamental attributes of traditional currency: they lack widespread acceptance as a means of transaction and they fail to maintain a stable value over time, among other factors⁴⁸. Instead, they are predominantly utilized as investment assets rather than serving as direct replacements for government-issued currencies.⁴⁹ One of the most significant concerns is the inherent volatility of cryptocurrencies, particularly Bitcoin, when compared to traditional fiat currencies. This volatility can pose risks for users and may hinder the widespread adoption of cryptocurrencies as a stable medium of exchange. Additionally, other challenges, such as the energy-intensive nature of Bitcoin mining and the associated environmental considerations, must

⁴⁵ Susan Athey, "5 Ways Digital Currency Will Change the World," World Economic Forum Agenda (Jan. 22, 2015)

⁴⁶ Nakamoto (2008), See Note 37

⁴⁷ Saifedean Ammous, "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation, and International Development," *The Journal of Private Enterprise* 3 (2015).

⁴⁸ James Chapman and Carolyn A. Wilkins, "Crypto 'Money': Perspective of a Couple of Canadian Central Bankers," Bank of Canada Staff Discussion Paper 2019-1 (Ottawa: Bank of Canada, February 2019).

⁴⁹ Alan MacNaughton et al, "Policy Forum: Editors' Introduction - The Tax Treatment of Cryptoassets" (2023) 71:1 Canadian Tax Journal 33.

also be acknowledged. These issues, along with the solutions offered by stablecoins, will be explored in greater detail in the following chapters.

- The Rise and Impact of DeFi, Bitcoin, and Cryptocurrencies.

The rapid ascent of DeFi, Bitcoin, and other cryptocurrencies marks a transformative shift in the financial landscape, underscoring their growing significance and potential to reshape traditional financial systems. Virtual currencies, crypto-currencies, or payment tokens fall within the category of crypto-assets. Crypto assets, also referred to as tokens, can be described as “private digital assets”, that:

- a) are registered on certain types of a digital distributed ledger secured with cryptography;
- b) are not issued or backed by a central bank or public authority, and
- c) can be employed for exchange and/or investment objectives and/or to obtain goods or services.⁵⁰

Within this expansive category, virtual currencies, exemplified by Bitcoin, serve as a versatile form of payment. Virtual currencies function as both a unit of account and a medium of exchange.⁵¹

Cryptocurrencies face limitations as legal tender, making their use for purchasing goods or services illegal in many jurisdictions⁵². Labeling these assets as "cryptocurrencies" is a significant issue and a misnomer. While cryptocurrencies can function as a medium of exchange, they are often not considered official currencies unless formally sanctioned by the central bank of a country. This is because, traditionally, the definition of currency includes official recognition and regulation by a government authority. However, the debate over what constitutes a currency is ongoing, particularly in regions like North America, where cryptocurrencies are not widely used as everyday currency despite their potential to be used in such a manner. The distinction between theoretical

⁵⁰ R. Houben and A. Snyers, 'Cryptoassets: Key Elements, Regulatory Concerns and Responses' (Study requested by the ECON Committee of the European Parliament, 2020) at 1-73.

⁵¹ Gabriella Gimigliano (2021), See note 15

⁵² David Sanz-Bas et al, “Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain” (2021) 10:3 *Laws* 57, online: <https://doi.org/10.3390/laws10030057>.

capability and actual practice is a significant factor in this classification.⁵³ Critics often argue that Bitcoin lacks "tangible" value, implying it should be deemed worthless⁵⁴. However, it's important to unpack what gives various forms of money their value. Others draw a parallel with gold, which possesses tangible value⁵⁵ due to its physical properties—scarcity, durability, and widespread acceptance as a store of value throughout history. Its value is also reinforced by the fact that it has been used as a medium of exchange and a benchmark for currencies.

In contrast, the US dollar, as a fiat currency, does not have intrinsic value in the same way gold does. Instead, its value is derived from its status as legal tender, meaning it is recognized and accepted for transactions by law. The US government's backing and the public's trust in the stability of the government and its institutions play crucial roles in maintaining the dollar's value. Bitcoin, on the other hand, lacks both tangible properties like gold and legal tender status like fiat currencies. Yet, it holds value for different reasons—primarily because of trust, utility, and societal consensus. Trust is established through the security of the blockchain, utility comes from its ability to facilitate decentralized transactions, and societal consensus emerges from the growing number of people who recognize and accept it as a form of value.

These differences highlight that the value of Bitcoin, much like fiat currencies and gold, is ultimately shaped by what people collectively believe it to be worth. The perception of value, whether rooted in physical properties, government backing, or decentralized technology, is a key factor in determining the viability of any currency. The characteristics of Bitcoin, specifically its scarcity and self-sovereignty, position it as a potential store of value and a potential safeguard against political and economic turmoil orchestrated by global governments. With the expansion of its network, the value proposition amplifies, driven by heightened trust and liquidity. While Bitcoin was initially conceived as a peer-to-peer currency, its deflationary attributes and fixed fees

⁵³ Ibid.

⁵⁴ Shawn Tully, "Is this a Bitcoin bubble? The debate is roiling some of Wall Street's most seasoned investors" *Fortune* (21 October 2021) online: <https://fortune.com/2021/10/21/is-this-a-bitcoin-bubble-the-debate-is-roiling-some-of-wall-streets-most-seasoned-investors/>.

⁵⁵ Ibid

act as deterrents for small-scale transactions. There are some beliefs (“some who believe” might be better) that bitcoin serves as the flagship of an emerging asset class, encompassing cryptocurrencies, with versatile applications.⁵⁶

Bitcoin, considered the pioneering and persistently dominant cryptocurrency, emerged as a techno-anarchist endeavor seeking to establish a digital alternative to conventional physical currency. The goal was to provide individuals with a means of conducting transactions free from potential interference by governments or banks. This virtual currency⁵⁷ operates as a self-sustaining cryptocurrency within a decentralized peer-to-peer system.

Ethereum (ETH), the second-largest cryptocurrency with a market cap of \$230 billion, was conceptualized by Vitalik Buterin in 2014 and mined its first block in 2015. Functioning as an extension of Bitcoin's applications, Ethereum introduced smart contracts, enabling code on a blockchain to control assets, data, and interactions among network participants. This innovation gave rise to DApps, eliminating the need for a central clearinghouse and fostering direct peer-to-peer interactions⁵⁸. Financial DApps quickly led to the movement known as DeFi. The cryptocurrencies sector has transitioned its emphasis away from delivering payments to providing an extensive array of financial services. This fresh suite of financial offerings experienced a substantial rise in popularity commencing approximately in 2020. These services are primarily accessible on an alternative blockchain, notably Ethereum.⁵⁹

In the absence of a trusted intermediary, as is the case in the crypto domain, a smart contract assumes the role of custodian. A borrower typically borrows cryptocurrency or another digital asset and secures a separate digital asset within the smart contract as collateral. The release of this

⁵⁶ Harvey et al., 2021 See note 11 p.12

⁵⁷ See the definition of “Virtual Currency” Uniform Regulation of Virtual Currency Businesses Act, s 23, online: <https://www.cga.ct.gov/2018/TOB/h/2018HB-05496-R00-HB.htm> (accessed January 25, 2024). Raised Bill No. 5496, February Session, 2018, LCO No. 2228; defines a “virtual currency” as “a digital representation of value that is used as a medium of exchange, a unit of account, or a store of value; and is not legal tender...” The Uniform Regulation of Virtual Currency Businesses Act (URVCBA) had been proposed by the Uniform Law Commission (ULC) to provide a model framework for the regulation of virtual currency businesses.

⁵⁸ Chris Brummer (2022) See note 5

⁵⁹ For the most recent observation, refer to the source: DeFiLama (<https://defillama.com/chain/Ethereum?currency=USD>) Last observation: January 17, 2024

collateral is contingent upon the borrower's repayment of the loan. In the event of a borrower default, the smart contract autonomously transfers the collateral to the lender or liquidates it to reimburse the lender, depending on the terms of the contract. The automatic execution of smart contracts, driven by pre-established conditions, mitigates incentive-related challenges that a conventional intermediary might encounter⁶⁰.

The decentralization of cryptocurrencies restricts the ability of governments to exert control over them. As a result, cryptocurrencies are not confined to any specific geographical region and can be exchanged globally. Consequently, Bitcoin, for instance, proves valuable for facilitating cost-effective international money transfers. This is particularly beneficial for individuals sending smaller sums of money, such as remittance payments—funds sent by migrants to support family members in their home countries⁶¹. Traditional remittance services often charge high fees, especially for small amounts, but Bitcoin allows these transfers to be made quickly and at a lower cost, making it an attractive alternative for people who rely on sending remittances regularly. This form of transfer is often more economical compared to transactions involving central bank-issued currencies, as cryptocurrencies enable worldwide financial transfers without the necessity of an intermediary institution. Furthermore, the elimination of intermediaries enhances the speed of money transfers⁶².

Another facet of cryptocurrencies is their contribution to financial inclusion, as they do not necessitate sophisticated technological infrastructure beyond access to the internet and a digital device, such as a smartphone, for transactional engagement. Additionally, the supply of cryptocurrencies remains immune to government or central bank influence, as it is predetermined by the underlying protocol of the cryptocurrency⁶³. Consequently, no state can manipulate the

⁶⁰ Jonathan Chiu & Hanna Yu, "Decentralized Finance: Innovations and Challenges," Bank of Canada Staff Analytical Note 2023-15, October 2023, online: <https://www.bankofcanada.ca/2023/10/staff-analytical-note-2023-15/>

⁶¹ Brett Scott, "How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?" (2016) UNRISD Working Paper No. 2016-1 (United Nations Research Institute for Social Development, Geneva).

⁶² Moritz Holtmeier and Philipp Sandner, "The Impact of Cryptocurrencies on Developing Countries" (December 2019), Frankfurt School Blockchain Centre Working Paper.

⁶³ Nakamoto (2008), See note 37.

money flow, thereby constraining governmental authority. On one hand, this may be seen as favorable, since it promotes financial autonomy by limiting government control over currency. On the other hand, it challenges traditional monetary policies and potentially undermines government authority in economic matters.

In the realm of financial systems, a longstanding paradigm of centralization has prevailed, with central banks wielding authority over the money supply and financial transactions primarily mediated by intermediaries. This conventional model, characterized by the dominance of localized banks and traditional banking institutions, has presented inherent challenges. However, the landscape has witnessed a transformative shift in recent years with the emergence of DeFi, a paradigm wherein peer-to-peer interactions unfold on a shared ledger free from centralized control. In their collaborative work titled "DeFi and the Future of Finance" published in 2021, Campbell R. Harvey, along with Ashwin Ramachandran and Joey Santoro⁶⁴, shed light on the significant potential of DeFi in addressing five pivotal issues ingrained in centralized financial systems.

Firstly, the issue of centralized control pervades various layers, wherein consumers and businesses find themselves tethered to a singular localized bank exercising control over rates and fees. Switching institutions is feasible but often incurs substantial costs, accentuating the concentrated nature of the banking system. Beyond traditional finance, newer tech giants like Amazon, Facebook, and Google wield concentrated influence in specific industries, compounding the challenges associated with centralized control.

The second predicament, limited access, plagues approximately 1.7 billion unbanked individuals, posing barriers to obtaining loans and participating in online commerce. Even among the banked population, access remains uncertain, with financial institutions potentially unwilling to entertain small loans vital for emerging businesses.

⁶⁴ Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro, *DeFi and the Future of Finance* (April 5, 2021), available at <https://compoundmaven.com/wp-content/uploads/2022/08/DeFi-And-The-Future-Of-Finance-Duke-University-August-2021.pdf>.

The reliance on credit card loans with exorbitant borrowing rates highlights the significant challenges entrepreneurs face in securing affordable financing to build and sustain their businesses. Harvey et al. emphasize the lack of guarantee for access even for those within the banking system, exemplifying instances where banks may steer businesses towards credit card loans with exorbitant borrowing rates exceeding 20% annually⁶⁵.

Inefficiency, the third obstacle, permeates centralized financial systems, manifesting in practices such as the credit card interchange rate, which extracts up to 3% of a transaction's value with each swipe. Remittance fees stand at 5-7%, and antiquated settlement times for stock transactions persist, highlighting the systemic inefficiencies. These include sluggish fund transfers, brokerage fees, security concerns, and limitations on microtransactions, all contributing to a less-than-optimal user experience. In the existing banking system, low deposit interest rates and high loan interest rates persist due to the need to offset brick-and-mortar expenses, echoing similar challenges in the insurance industry.

Lack of interoperability, the fourth challenge, ensnares consumers and businesses within a siloed financial environment designed to uphold high switching costs. Initiatives, such as Visa's attempted acquisition of Plaid, seek to alleviate these issues but often fall short of addressing fundamental flaws in the overarching financial infrastructure⁶⁶. The struggle to move money swiftly and seamlessly between institutions persists, exemplified by the protracted timelines associated with wire transfers. Notably, the limited competition in the digital financial services market, particularly in traditional payment systems, is largely due to the exclusive control that established payment providers have over transaction information and the general lack of interoperability between different systems⁶⁷. This low market contestability, where new entrants

⁶⁵ Ibid

⁶⁶ Frédéric Marty & Thierry Warin, Visa's Abandoned Plan to Acquire Plaid: What Could Have Been a Textbook Case of a Killer Acquisition, CIRANO Scientific Paper No 2021S-39, online: <https://cirano.qc.ca/files/publications/2021s-39.pdf>.

⁶⁷ European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Decentralized finance – Information frictions and public policies – Approaching the regulation and supervision of decentralized finance, Publications Office of the European Union (2022), online: <https://data.europa.eu/doi/10.2874/444494>.

struggle to compete, presents a significant challenge in the context of DeFi regulation, where fostering a more open and competitive environment is crucial⁶⁸. However, there are contrasting beliefs regarding interoperability in the DeFi space. While many argue that DeFi protocols can be easily combined and interfaced to create new solutions,⁶⁹ others express concerns about the potential challenges, such as technical incompatibilities or lack of standardization, which could hinder seamless interoperability. Despite these concerns, the inherent ability to freely interoperate digital services and connect protocols in DeFi largely stems from their open and public nature, a characteristic inherited from the tradition of open-source systems in computer science. This dynamic has no direct equivalent in the traditional financial system⁷⁰.

The fifth problem, opacity, characterizes the current financial system's lack of transparency. In jurisdictions like the United States, for example, bank customers often contend with limited insights into their bank's financial health, relying heavily on Federal Deposit Insurance Corporation (FDIC) insurance for protection. The fragmented nature of the loan market makes it challenging to seek competitive loan rates, exacerbating inefficiencies inherent in the system. While Fintech services have made strides in improving consumer insurance and access to financial products, they remain constrained by legacy costs and bloated back-office expenses⁷¹. It's important to note that these issues may manifest differently across jurisdictions, such as in Canada, where the banking sector is more consolidated and regulated. Therefore, while the broad points made here apply in many contexts, the specific challenges and solutions can vary depending on the jurisdiction.

These five challenges have far-reaching implications, impeding economic growth and deterring high-quality investment projects. Elevated loan rates stemming from legacy costs may discourage entrepreneurs from pursuing economically promising projects, hindering overall

⁶⁸ Ibid

⁶⁹ Ibid

⁷⁰ Ibid

⁷¹ Harvey et al. (2021), See note 32.

economic acceleration⁷². While it's true that borrowing costs have been historically low for governments and individuals with substantial means, this accessibility has not been uniformly experienced across all sectors. Entrepreneurs and small businesses often face higher borrowing costs due to risk premiums and less favorable loan terms, making it more difficult for them to capitalize on growth opportunities⁷³.

One major challenge in the current financial system is the persistence and deepening of inequality. While there is widespread agreement on the need for equal opportunity, views on achieving it differ. It is generally believed that funding should be based on the merit of a project and its execution, rather than external factors. However, inequality remains a significant barrier, preventing promising ideas from being realized, especially due to issues like limited access to traditional banking and reliance on costly alternatives. These challenges hinder the creation of a fair financial system. Despite technological advancements, the centralized financial system has yet to fully utilize them. In contrast, DeFi offers a potential solution, presenting an opportunity to reshape the financial landscape towards a more inclusive and equitable future.⁷⁴

However, the assertion that DeFi contributes to financial inclusion is somewhat questionable. Because those without traditional bank accounts often possess smartphones, enabling financial transactions via smartphones without a bank account could ostensibly enhance financial inclusion. Nonetheless, there are two primary concerns.⁷⁵ Firstly, concerns about 'Competent Knowledge and Literacy' are evident. Simply owning a smartphone does not ensure that users can engage in DeFi transactions productively, wisely, or knowledgeably⁷⁶. DeFi typically demands a high level of expertise and literacy, which could widen the gap between those proficient in DeFi and those not. This factor is particularly pertinent given the nascent nature of

⁷² Ibid.

⁷³ N Huyghebaert, "The Capital Structure of Business Start-Ups: Policy Implications" (2003) 48:1 *Tijdschr Econ en Manag*, online: <https://lirias.kuleuven.be/retrieve/12808>.

⁷⁴ Ibid, p. 7

⁷⁵ Tomonori Yuyama, Ken Katayama & Paul Brigner, "Proposal of Principles of DeFi Disclosure and Regulation," in A. Essex et al. (eds.), *Financial Cryptography and Data Security. FC 2023 International Workshops. FC 2023. Lecture Notes in Computer Science*, vol 13953 (Springer, Cham, 2024), pp. 141–164, https://doi.org/10.1007/978-3-031-48806-1_10.

⁷⁶ Ibid

DeFi technology⁷⁷. Secondly, current DeFi usage is constrained. Even if DeFi transactions were feasible via smartphones, they are mostly focused on cryptocurrency trading. While DeFi is sometimes used to reduce the high fees associated with sending money across borders, its overall use is still limited.⁷⁸

Despite its transformative potential, DeFi faces challenges, including regulatory uncertainties, security risks, and the need for industry standards. Collaborative efforts among developers, regulators, and users are imperative for sustained growth. On the global regulatory front, authorities grapple with the rise of DeFi, acknowledging its innovation and inclusivity while navigating unique challenges posed by its decentralized nature. The ongoing regulatory task involves balancing innovation with effective risk mitigation strategies to ensure the stability and legitimacy of the evolving DeFi ecosystem.

⁷⁷ Ibid, pp. 141–164,

⁷⁸ Ibid

Chapter IV: Regulatory Challenges and Concerns

To effectively develop or revise policies for new technologies, it is crucial to understand their roles in the economy and society, a challenge intensified by blockchain's borderless, global nature⁷⁹. Partially in reaction to the drawbacks associated with crypto assets—such as their price volatility, potential for facilitating illicit activities, lack of consumer protections, and environmental concerns related to energy-intensive mining practices—and partially due to the rapid expansion of the crypto industry, there is a rising trend among governments and international bodies to impose regulations, standardize practices, and levy taxes on transactions involving crypto assets.⁸⁰ Although the utilization of payment tokens remains a specialized area, the economic and legal literature has exhibited significant interest in this subject since the release of Satoshi Nakamoto's manifesto. Legal scholars primarily concentrate on:

- determining the legal classification of crypto assets, including whether they can be compared to investment instruments, funds, securities, or intangible assets, in order to identify the most appropriate rules and regulations among those currently in effect.⁸¹
- the negative and positive facets of the decentralized crypto-governance system⁸²;
- the potential financial stability and reputational risks linked to incorporating the crypto system into conventional banking and financial structures⁸³.

In many jurisdictions, categorizing cryptocurrencies as either securities or commodities leads to compliance challenges related to registration requirements for securities or commodities, broker-dealer registration, fraud liability, and disclosure obligations. This classification

⁷⁹ Catherine Mulligan, Suzanne Morsfield & Evîn Cheikosman, "Blockchain for sustainability: A systematic literature review for policy impact" (2024) 48:2 Telecommunications Policy 102676, online: ScienceDirect <https://doi.org/10.1016/j.telpol.2023.102676>.

⁸⁰ Alan MacNaughton et al. (2023) See note 49.

⁸¹ Benjamin Geva, 'Cryptocurrencies and the Evolution of Banking, Money, and Payments,' in C. Brummer ed, *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (Oxford: Oxford University Press, 2019) at 20-22; Noah Vardi, 'Bit by Bit: Assessing the Legal Nature of Virtual Currencies,' in G. Gimigliano ed, *Bitcoin and Mobile Payments: Constructing a European Union Framework* (London: Palgrave-Macmillan, 2016) at 60-66.

⁸² Hossein Nabilou, 'Bitcoin Governance as a Decentralized Financial Market Infrastructure' (2020) 4(2) *Stanford Journal of Blockchain Law and Policy* 177-202 at 180-185.

⁸³ Angela Walch, "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems," in *Crypto Assets: Legal and Monetary Perspectives*, edited by Chris Brummer (Oxford: Oxford University Press, 2019), <https://doi.org/10.1093/oso/9780190077310.003.0003>.

significantly impacts the operational, compliance, and profitability aspects of cryptocurrency businesses. Numerous countries, such as the USA, appear to regulate cryptocurrencies as securities. The prevailing view suggests that cryptocurrencies are hybrid intangibles, functioning as either securities or commodities,⁸⁴ depending on their specific characteristics. In the U.S., the Securities and Exchange Commission (SEC) tends to classify a cryptocurrency as a security if it meets the criteria of the Howey Test, which assesses whether a transaction involves an investment of money in a common enterprise with an expectation of profit derived from the efforts of others⁸⁵. For example, initial coin offerings (ICOs), which are the equivalent of an initial public offering (IPO) in the cryptocurrency industry, often fall under this category because they involve raising capital from investors with the promise of future returns. Canada also tends to follow this approach, (employing a test like the U.S. Supreme Court's Howey Test, as seen in *OSC v. Pacific Coast Coin Exchange*), to classify digital assets, and similarly treats certain cryptocurrencies as commodities, a topic that will be explored further in subsequent chapters. Meanwhile, the Commodity Futures Trading Commission (CFTC) in the U.S. may classify a cryptocurrency as a commodity under the Commodity Exchange Act⁸⁶, if its primary function is as a medium of exchange, store of value, or unit of account, akin to traditional commodities like gold or oil⁸⁷. Bitcoin and Ethereum, for instance, are typically classified as commodities because they are decentralized and primarily function in roles like medium of exchange or store of value, rather than serving as investments dependent on a central authority's efforts. The SEC's regulation of cryptocurrencies differs depending on the unique characteristics of each digital asset. This dynamic and multifaceted

⁸⁴ See: *SEC vs. Life Partners*, 87 F3d 536 (CA8, 1996). See: *First Financial Federal vs. E. F. Hutton Mortgage Corporation*, 834 F2d 685 (CA8, 1987). See: *Revak vs. SEC Realty Corp.*, 18 F3d 81 (CA2, 1994). See: *Banco Espanol De Credito vs. Security Pacific National Bank*, 973 F2d 51 (cert. Den.) 509 US 903. See: *Perez-Rubio vs. Wyckoff*, 718 Fsupp 217 (1989). See: *Developer's Mortgage Co. vs. Transohio Savings Bank*, 706 FSupp. 570 (1989). See: *Matell vs. Maturat*, 862 F2d 720 (CA9, 1988). See: *Giuffre Organization vs. Euromotor Sport Racing*, 141 F3d 1216 (CA7, 1998). See: *Klaers v. St Peter*, 942 F2d 535 (CA8, 1991). See: *Peeves vs. Teuscher*, 881 F2d 1495 (CA9, 1989). See: *SEC vs. ETS Payphone*, 408 F3d 727 (CA11, 2005).

⁸⁵ *SEC v WJ Howey Co*, 328 US 293 (1946).

⁸⁶ *Commodity Exchange Act*, 7 USC § 1 (1936).

⁸⁷ U.S. Commodity Futures Trading Commission, *An Introduction to Virtual Currency* (February 2018), online: CFTC

https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/oceo_aivc0218.pdf

regulatory framework highlights the difficulties in categorizing cryptocurrencies within existing legal boundaries.

Numerous nascent challenges in safeguarding investors and consumers arise within the realm of cryptocurrencies⁸⁸. Although DeFi protocols offer transparency and operate in a 'trustless' manner, these features alone may not be sufficient to fully protect users. There is often a lack of incentives for developers to provide comprehensive disclosures about potential risks, governance structures, or the underlying code. This underscores the necessity for mandating disclosure requirements and business registration obligations, particularly for DeFi lending protocols and algorithmic stablecoins⁸⁹, to ensure that users have a clear understanding of the risks involved and can make informed decisions. Standardized guidelines concerning the promotion of cryptocurrencies and DeFi, including endorsements by celebrities and social media influencers, remain undefined throughout Canada⁹⁰. The U.S. Securities and Exchange Commission (SEC) has demonstrated a readiness to pursue enforcement measures against celebrities and entrepreneurs for unlawfully promoting crypto assets.⁹¹

The future growth and acceptance of cryptocurrencies hinge on effective regulation that defines the extent of freedoms and advantages these digital currencies can retain. Striking a careful balance in the regulation of cryptocurrencies is essential. While one of the key benefits of cryptocurrencies is their lack of centralization, political support is still necessary to ensure the broader acceptance and integration of these technologies within existing legal and financial frameworks. Effective regulation that garners political support⁹² can help protect consumers, prevent misuse, and foster a stable environment where cryptocurrencies can thrive without

⁸⁸ Caroline Crenshaw, "DeFi Risks, Regulations, and Opportunities" (2021) 1 *Intl. J. Blockchain L.* at 4.

⁸⁹ *Ibid*

⁹⁰ Ryan Clements, "Emerging Canadian Crypto-Asset Jurisdictional Uncertainties and Regulatory Gaps" (2021) 37(1) *Banking & Finance L. Rev.* at 36-40, 47-52.

⁹¹ U.S. Securities and Exchange Commission, "SEC Charges Crypto Entrepreneur Justin Sun and His Companies for Fraud and Other Securities Law Violations: Eight Celebrities Also Charged for Illegal Touting of Sun's Crypto Asset Securities" (22 March 2023), online: SEC <www.sec.gov/news/press-release/2023-59>.

⁹² Moritz Holtmeier and Philipp Sandner (2019) See note 62.

undermining their decentralized nature. Only with political backing can there be widespread adoption of cryptocurrencies⁹³. The challenge lies in crafting regulations that support these goals without imposing excessive central control. In contrast to the decentralization of telecommunication networks, blockchain-based communication systems can be implemented without intermediaries, making it difficult for governments to impose regulations akin to those on traditional networks, except through an unenforceable prohibition of the technology's usage⁹⁴.

At present, political backing for cryptocurrencies is generally lacking due to concerns about fraud and the potential loss of control over economic policies, such as monetary policy⁹⁵. Consequently, various countries have taken measures to restrict the use of cryptocurrencies⁹⁶. For instance, in 2021, China has imposed a blanket ban on cryptocurrency trading and mining, citing concerns over financial stability and the environment and the perceived threat that cryptocurrencies pose to the sovereign digital yuan⁹⁷. India has also proposed legislation to ban cryptocurrencies, although the legal status remains in flux⁹⁸. On the other hand, the European Union has introduced the Markets in Crypto-Assets (MiCA) regulation, aiming to create a regulatory framework that mitigates risks while allowing innovation⁹⁹. These measures reflect a spectrum of approaches, from outright bans to more regulated environments. However, enforcing such measures can be challenging due to the decentralized and borderless nature of cryptocurrencies, which often operate outside the traditional financial systems. While countries can impose regulations within their borders, the global and decentralized nature of

⁹³ Christian Jaag and Christian Bach, "Cryptocurrencies: New Opportunities for Postal Financial Services" (2015) Working Papers 0052, Swiss Economics.

⁹⁴ Aaron Wright & Primavera De Filippi (2015), see note 27, p.23

⁹⁵ Expert Group on Regulatory Obstacles to Financial Innovation (2019), see note 14.

⁹⁶ Moritz Holtmeier and Philipp Sandner (2019) See note 62.

⁹⁷ Reuters, "Chinese Financial, Payment Bodies Barred from Cryptocurrency Business" (18 May 2021), online: <https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/>

⁹⁸ Deshant Singh Thakur, Raj A Varma & Damodar Mayappa Hake, "Regulation of Cryptocurrency in India: Issues and Challenges" (2022) 6:5 J Positive School Psychol, online: <https://journalppw.com/index.php/jpsp/article/view/9707/6356>.

⁹⁹ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, online: EUR-Lex <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>.

cryptocurrencies means that complete control or prohibition may be difficult to achieve in practice¹⁰⁰.

The apprehension about relinquishing control arises from the inability of national governments to regulate cryptocurrencies and, consequently, their money supply, which could result in a compromise of financial sovereignty. This concern has led some governments to explore the introduction of central bank digital currencies (“CBDC”s) as a potential solution¹⁰¹. While the primary benefit of cryptocurrencies is their independence from central banks and government control, CBDCs are proposed to retain some of the technological advantages of digital currencies—such as efficiency and security—while allowing governments to maintain control over monetary policy and financial stability¹⁰². Essentially, CBDCs represent a way for governments to address the challenges posed by unregulated cryptocurrencies by offering a regulated alternative that aligns with their economic and financial objectives. Currently, Canada lacks a functioning CBDC. The Bank of Canada is actively researching the development and implementation of a CBDC as a potential measure to address or preempt the negative network effects and reduction in the use of physical currency caused by the widespread adoption of privately issued stablecoins as substitutes for money in consumer transactions¹⁰³. The Bank of Canada is exploring various aspects of CBDCs such as their design, core features, underlying principles, and potential models¹⁰⁴, driven partly by the decreased acceptance of physical fiat currency by merchants, which has been accelerated by the COVID-19 pandemic¹⁰⁵. Additionally,

¹⁰⁰ Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu & Adefolake Olachi Adewusi, "International Enforcement of Cryptocurrency Laws: Jurisdictional Challenges and Collaborative Solutions" (2024) 11:2 Magna Sci Adv Res Rev, online: <https://doi.org/10.30574/msarr.2024.11.1.0075>.

¹⁰¹ Christine Lagarde (ed), *Winds of Change: The Case for New Digital Currency* (International Monetary Fund, 2018).

¹⁰² Tommaso Mancini-Griffoli et al, *CASTING LIGHT ON CENTRAL BANK DIGITAL CURRENCY* (November 2018), IMF Staff Discussion Note SDN/18/08, online: IMF <https://www.imf.org/-/media/Files/Publications/SDN/2018/SDN1808.ashx>.

¹⁰³ Bank of Canada, "Contingency Planning for a Central Bank Digital Currency" (25 February 2020), online: Bank of Canada <www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/>.

¹⁰⁴ Bank of Canada, "The Positive Case for a CBDC" (20 July 2021), Staff Discussion Paper 2021-11; Bank for International Settlements, "Central Bank Digital Currencies: Foundational Principles and Core Features" (9 October 2020), online: BIS <www.bis.org/publ/othp33.htm>.

¹⁰⁵ Bank of Canada, "Payments Innovation Beyond the Pandemic, Remarks by Timothy Lane, Deputy Governor" Institute for Data Valorization (10 February 2021), online (pdf): Bank of Canada <www.bankofcanada.ca/wp-content/uploads/2021/02/remarks-2021-02-10.pdf>.

this exploration is motivated by concerns over the potential dominance of a privately issued fiat-backed stablecoin as a primary currency¹⁰⁶. Key concerns regarding CBDCs include privacy implications, design considerations, operational and cyber-security risks, as well as the extent of governmental surveillance or control they may entail¹⁰⁷. Some scholars believe that once DeFi ecosystems are appropriately regulated and supervised, central banks could bolster them by creating wholesale CBDCs with programmability similar to contemporary cryptocurrencies¹⁰⁸. This could address the trust issues associated with privately issued stablecoins¹⁰⁹ and serve as a trust anchor to support these markets, facilitating their growth¹¹⁰.

The staff note by Bank of Canada¹¹¹ highlights key challenges that limit the overall economic benefits of DeFi. The challenges include:

- Limited Tokenization: DeFi relies on tokenized assets recorded on the blockchain to interact with smart contracts. However, the note points out that only a few real-world assets have been tokenized. This limitation results in a self-referential system primarily focused on speculative crypto trades, contributing minimally to the real-world economy.
- High Concentration and Interconnectedness: The DeFi network, particularly on Ethereum, is depicted as increasingly interconnected over time. The system heavily relies on centralized stablecoins and the native token ETH, leading to concentration risks. Most values are locked into a few DeFi protocols, making the system vulnerable to operational or financial shocks to these key protocols, potentially causing system-wide spillover effects.

¹⁰⁶ Bank of Canada, "Money and Payments in the Digital Age, Remarks by Timothy Lane, Deputy Governor, CFA Montreal Fintech RDV2020" (February 2020), online (pdf): Bank of Canada <www.bankofcanada.ca/wp-content/uploads/2020/02/remarks-250220.pdf>.

¹⁰⁷ Andrea Tinianow & Stephen Palley, "A Round Table Discussion on Stablecoins: Taking the World By Storm or Storming the World?" (2022) 3 International Journal of Blockchain Law 4 at 9.

¹⁰⁸ Raphael Anton Auer, *Embedded Supervision: How to Build Regulation into Decentralised Finance* (St. Louis: CESifo, 2022), online: ProQuest <https://ezproxy.library.dal.ca/login?url=https://www.proquest.com/working-papers/embedded-supervision-how-build-regulation-into/docview/2675434688/se-2>

¹⁰⁹ J Frost, HS Shin & P Wierds, *An Early Stablecoin? The Bank of Amsterdam and the Governance of Money*, BIS Working Papers No 902 (2020).

¹¹⁰ R Auer & R Böhme, *The Technology of Retail Central Bank Digital Currency*, BIS Quarterly Review (March 2020) 85 at 100.

¹¹¹ Jonathan Chiu & Hanna Yu (2023), See note 60

- Unregulated CeFi: Despite DeFi's goal to eliminate centralized intermediaries, the note observes that retail users face challenges participating directly due to the specialized knowledge required. This has led to the emergence of unregulated centralized finance (CeFi) platforms¹¹², which operate differently from DeFi. CeFi platforms, run by people instead of smart contracts, expose investors to custodian risk and lack transparency. The recent bankruptcies of centralized platforms like Celsius and FTX underscore the associated risks with these unregulated CeFi entities¹¹³.

In summary, the Bank of Canada staff note emphasizes that, despite its innovative potential, DeFi faces limitations in tokenization, concentration risks, and the emergence of unregulated CeFi entities, impacting its broader economic benefits. These challenges warrant careful consideration when assessing the overall effectiveness and risks associated with the DeFi ecosystem.

Before enacting regulations, many nations observe the regulatory approaches of others, drawing insights and best practices from various jurisdictions. Europe, renowned for its proactive stance in regulating technological advancements and fostering innovation, serves as a leading example in shaping regulatory frameworks for emerging industries. In pursuit of enhancing legal certainty, ensuring the protection of crypto users, and upholding market integrity, The Markets in Crypto Assets Regulation (also referred as “MiCA”)¹¹⁴, enacted in June 2023, has been critiqued for its expansive yet incomplete definition of crypto assets. While MiCA’s broad approach aims to cover a wide range of digital assets, it falls short by failing to adequately include various innovative aspects of the decentralized finance (DeFi) ecosystem. Specifically, the regulation does not address certain DeFi applications, such as on-chain and algorithmic tokens, or DAOs, leaving these significant areas of the crypto landscape unregulated. By omitting these key elements, MiCA

¹¹² CeFi, or Centralized Finance, refers to traditional financial services provided through centralized institutions like banks and exchanges, where transactions and services are managed by a central authority. (Digital Assets, "Crypto Market Insights: 3 Key Differences Between DeFi and Centralized Finance Platforms" (15 May 2023), online: Forbes <https://www.forbes.com/sites/digital-assets/2023/05/15/crypto-market-insights-3-key-differences-between-defi-and-centralized-finance-platforms/>.)

¹¹³ Jonathan Chiu & Hanna Yu (2023), See note 60

¹¹⁴ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, online: EUR-Lex <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>.

may fall short of fully achieving its goals of legal certainty and market integrity, leaving significant parts of the crypto market unregulated. Additionally, MiCA does not implement supplementary measures, like an EU-based regulatory sandbox, which could have facilitated the development and testing of unregulated areas. This exclusion creates a gap in the regulatory framework, potentially hindering effective oversight and the integration of emerging crypto technologies.¹¹⁵

In Singapore on the other hand, the regulation of DeFi operates within the framework of existing financial legislation, primarily the Securities and Futures Act (“SFA”)¹¹⁶ and the Payment Services Act (“PSA”)¹¹⁷. Both laws were enacted in January 2020 to oversee payment services, including cryptocurrency-related activities. Under the PSA, e-money-based payment services and digital payment token services are specifically regulated. Additionally, cryptocurrencies and related trades may fall under the definition of a "capital market product" subject to regulation under the SFA. Token issuers are mandated to obtain licenses corresponding to their cryptocurrency activities, unless exempted under the SFA.

Decentralized exchanges in Singapore are classified as "organized markets" under the SFA, necessitating approval or recognition by the Monetary Authority of Singapore (MAS) if identifiable. However, in cases where the market cannot be identified or linked to a regulated entity, there are currently no overarching regulations in place. Although there are no direct regulations targeting DeFi in Singapore, MAS is actively monitoring the sector and utilizing regulatory sandboxes to gain insights and understanding. For instance, InvestaX introduced its exchange in the MAS sandbox in September 2021, including a DeFi platform named IX Swap, reflecting ongoing efforts to engage with emerging financial technologies.

DeFi regulation might be difficult as it has specific risks and challenges that regulators need to consider, and public consultation is very important for this reason. Additionally, the

¹¹⁵ Gabriella Gimigliano (2021), See note 15

¹¹⁶ Securities and Futures Act 2001, online: Singapore Statutes Online <https://sso.agc.gov.sg/Act/SFA2001>.

¹¹⁷ Payment Services Act (PSA) 2019, online: Monetary Authority of Singapore <https://www.mas.gov.sg/regulation/acts/payment-services-act>.

dynamic and innovative nature of DeFi necessitates a flexible regulatory approach that can adapt to rapid technological changes. Traditional regulatory frameworks may struggle to keep pace with these advancements, highlighting the need for ongoing dialogue between regulators, industry participants, and the public to ensure that regulations remain effective and relevant. Subsequent sections of the thesis will discuss those challenges and risks related to the DeFi ecosystem.

Chapter V: Fintech and Financial Regulations – Can DeFi be regulated?

Regulatory concerns regarding decentralized finance (DeFi) are addressed in Analytical Notes published by the Bank of Canada¹¹⁸. Currently, DeFi poses limited risks to financial stability, yet its potential links to the real economy may grow over time. Numerous vulnerabilities in DeFi closely resemble those found in the traditional financial system, including run risk associated with stablecoins, leverage inherent in DeFi lending, and the interconnectedness among various protocols. Furthermore, DeFi introduces new challenges specific to blockchain technology, such as the emergence of new points of failure when blockchains interact with each other or with the real world¹¹⁹. For instance, when blockchains connect through cross-chain bridges, they can become vulnerable to security breaches, which has been demonstrated by several major bridge hacks¹²⁰. Additionally, interactions with external systems via oracles—which provide blockchains with data from the real world—can create additional risks. If an oracle supplies incorrect data, it could result in significant financial losses or manipulation within DeFi platforms¹²¹. Additionally, novel amplification channels, like flash loans, enable malicious actors to secure substantial funding, amounting to billions of dollars, without undergoing credit checks or collateral requirements.¹²² Due to the pseudonymity of blockchain users, most DeFi protocols do not involve traditional credit assessments. These Flash Crypto loans commonly necessitate overcollateralization as a prerequisite for extension, thereby limiting access to loans for individuals lacking sufficient wealth in the form of collateral¹²³. The anonymous and borderless nature of public blockchains adds complexity to regulatory oversight.¹²⁴

¹¹⁸ Jonathan Chiu & Hanna Yu (2023), See note 60

¹¹⁹ Jonathan Chiu & Hanna Yu (2023) see footnote 60

¹²⁰ Shaofei Lu et al, "CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle" (2023) 23:4 *Sensors* 1864, online: <https://doi.org/10.3390/s23041864>.

¹²¹ Ibid

¹²² *Hong Kong Institute for Monetary and Financial Research, Decentralised Finance: Current Landscape and Regulatory Developments* (June 2024), HKIMR Applied Research Report No 1/2024, online: <https://www.aof.org.hk/docs/default-source/hkimr/applied-research-report/defirep.pdf>.

¹²³ Sirio Aramonte et al., "DeFi Risks and the Decentralization Illusion," *BIS Quarterly Review*, no. 27 (December 2021), 27.

¹²⁴ Jonathan Chiu & Hanna Yu (2023) see note 60

Smart contracts function as programmable instructions, allowing them to be designed to manage specific tasks or activities such as buying or selling cryptocurrencies, or issuing payouts in gaming applications¹²⁵. Since smart contracts are self-executing, DApps, which are composed of these smart contracts, operate autonomously and are not controlled by any centralized authority¹²⁶. Instead of dealing with intermediaries who might exploit informational or other advantages, users engage directly with the protocol. Using smart contracts, developers who work with open-source and publicly available code can link to various applications, such as financial Application Programming Interfaces (“APIs”). This allows for a level of composability—meaning the ability to easily combine different financial components or protocols to create new products and services—that traditional finance cannot achieve.¹²⁷

The magnitude of systemic risk stemming from crypto-assets is influenced by familiar factors observed in traditional finance, such as leverage, duration and liquidity mismatches, opacity, and interconnections¹²⁸. The degree of systemic risk also hinges on the interplay between the cryptocurrency market and the broader financial system, including the extent of leverage within the financial landscape and the resilience of the system during market downturns and the unwinding of leverage positions¹²⁹. Furthermore, systemic risks arising from leverage and volatility associated with crypto-assets are contingent on whether these pressures remain contained within the crypto-ecosystem or spill over into the traditional financial realm, a scenario more likely if crypto-assets are widely held or utilized for payments, collateralized lending, and deposits¹³⁰.

¹²⁵ Ethereum Explanatory Document, "Introduction to Dapps," ETHEREUM, accessed January 1, 2024, <https://ethereum.org/en/developers/docs/dapps>.

¹²⁶ Chris Bummer (2022), see note 57

¹²⁷ Lily Francus, "Block by Block: Assessing Risk in Decentralized Finance," Moody's Analytics: Credit Where Due Blog Series (January 2022) available at https://www.moodyanalytics.com/articles/2021/block_by_block_assessing_risk_in_decentralized_finance..

¹²⁸ Ryan Clements & Virginia Torrie, "Crypto Asset Regulation in Canada: Developments and Governance Considerations," *Banking & Finance Law Review*, vol. 39, no. 3, (August 2023), pp. 345-380.

¹²⁹ Jon Cunliffe, "Is 'Crypto' a Financial Stability Risk?" (speech delivered at Bank of England, London, 13 October 2022), online: Bank of England <www.bankofengland.co.uk/speech/2021/october/jon-cunliffe-swifts-sibos-2021>.

¹³⁰ International Monetary Fund, "The Crypto Ecosystem and Financial Stability Challenges" (October 2021), online: IMF <www.imf.org/-/media/Files/Publications/GFSR/2021/October/English/ch2.ashx> at 44-45.

Thus far, it appears that crypto-systemic risk has remained confined to the crypto-ecosystem, with limited exposures for banks¹³¹. The recent events underscore uncertainties regarding the long-term sustainability of cryptoassets in the absence of adequate regulatory oversight, especially concerning fiat-referenced cryptoassets, commonly termed stablecoins¹³². The Bank of Canada found out that these occurrences have had minimal repercussions on Canada's financial system, which has limited linkages to crypto asset markets. This reinforces the Bank's stance that, presently, crypto asset markets do not pose a systemic risk to the Canadian financial system¹³³. However, as crypto assets continue to integrate into the financial system, there is a growing need for expedited progress in formulating regulations aimed at mitigating potential risks to financial stability, both domestically and internationally. Despite the rapid expansion of crypto asset markets in recent years, they remain relatively small compared to the global financial sector, thus not yet presenting a systemic threat¹³⁴.

Given the potential for widespread adoption of crypto-assets and stablecoins as consumer payment instruments, there are concerns about the associated financial stability risks. Specifically, crypto-asset markets may pose payment settlement risks if these digital assets gain traction in everyday transactions.¹³⁵ A dominant stablecoin issuer, accumulating substantial off-chain collateral reserves, could evolve into a global systemically important financial institution, thereby amplifying these risks¹³⁶. In response to these potential threats, regulatory authorities, such as the Bank of Canada and the Canadian Minister of Finance, might consider designating programmable blockchains or widely held stablecoin issuers as systems requiring extensive oversight under

¹³¹ Financial Times, "Can Crypto Contagion Infect Mainstream Finance?" (30 June 2022), online: FT <www.ft.com/content/03bb9296-b645-4311-abb2-14bc3ab66443>.

¹³² Bank of Canada, "Financial System Review—2023," accessed May 12, 2024, <https://www.bankofcanada.ca/2023/05/financial-system-review-2023/>.

¹³³ Ibid.

¹³⁴ Ibid.

¹³⁵ Fabian Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets" (15 April 2021), 103(2) Rev. Second Q. Economic Research, Federal Reserve Bank of St. Louis, online: St. Louis Fed. <research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets>.

¹³⁶ Timothy G. Massad, "Facebook's Libra 2.0: Why You Might Like It Even if We Can't Trust Facebook" (June 2020), online (pdf): Economic Studies at Brookings <www.brookings.edu/wp-content/uploads/2020/06/ES-6.22.20-Massad-1.pdf>.

applicable legislation.¹³⁷ Such designations could subject stablecoin issuers to stringent restrictions¹³⁸. Additionally, the Canadian Securities Administrators (“CSA”) has officially registered numerous cryptocurrency trading platforms as dealers¹³⁹. In February 2023, the CSA made an announcement stating that new cryptocurrency firms intending to register must adhere to stringent criteria aimed at safeguarding investors¹⁴⁰. The initial set of requirements includes restrictions on clients purchasing or depositing fiat-referenced crypto assets without obtaining prior written consent from the CSA.

Regulatory measures have been implemented by the Office of the Superintendent of Financial Institutions (“OSFI”)¹⁴¹ to curb bank exposures to cryptocurrencies, bolstered by regulatory capital and liquidity standards¹⁴². Crypto assets may introduce novel systemic dynamics extending beyond mere transactional aspects of finance, given their capacity to synthesize financial interests and amplify trading speed and volume¹⁴³. The proliferation of leverage in the financial system exacerbates fragility, leading to pro-cyclical pressures during crises and heightened volatility¹⁴⁴.

Moreover, the crypto-asset market exhibits notable concentration risk, particularly evident in the dominance of Binance in crypto-asset spot trading¹⁴⁵. A considerable portion of Bitcoin

¹³⁷ Payment Clearing and Settlement Act, S.C. 1996, c. 6, Sch., s. 4(1) [PCSA].

¹³⁸ Canadian Payments Act, R.S.C. 1985, c. C-21, at s. 37(1).

¹³⁹ Canadian Securities Administrators, "Crypto Trading Platforms Authorized to Do Business with Canadians," accessed May 12, 2024, <https://www.securities-administrators.ca/crypto-trading-platforms-regulation-and-enforcement-actions/crypto-trading-platforms-authorized-to-do-business-with-canadians/>.

¹⁴⁰ Canadian Securities Administrators, "CSA Staff Notice 21-332 Crypto Asset Trading Platforms: Pre-Registration Undertakings—Changes to Enhance Canadian Investor Protection" (February 22, 2023).

¹⁴¹ Office of the Superintendent of Financial Institutions, "Prudential Treatment of Crypto Asset Exposures" (5 July 2021), online: OSFI <www.osfi-bsif.gc.ca/Eng/fi-if/inai/Pages/prucrypt.aspx>.

¹⁴² Office of the Superintendent of Financial Institutions, "Interim Arrangements for the Regulatory Capital and Liquidity Treatment of Crypto Asset Exposures" (18 August 2022), online: OSFI <www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/crypto22.aspx>.

¹⁴³ Saule T. Omarova, "New Tech v. New Deal: Fintech as a Systemic Phenomenon" (2019) 36(2) *Yale J. on Regulation* 36.

¹⁴⁴ Hilary J. Allen, *Driverless Finance: Fintech's Impact on Financial Stability*, (Oxford: Oxford University Press, 2022).

¹⁴⁵ Helene Braun, "Binance Controlled 92% of Bitcoin Spot Trading Volume at End of 2022: Arcane Research" (4 January 2023), online: CoinDesk <www.coindesk.com/markets/2023/01/04/binance-controlled-92-of-bitcoin-spot-trading-volume-at-end-of-2022-arcane-research/>.

holdings is concentrated among miners, early adopters, and exchanges¹⁴⁶, with a significant proportion linked to a small fraction of digital wallet addresses¹⁴⁷. Concerns have been raised by the Bank for International Settlements regarding the ability of crypto-asset miners to influence transactions and extract value in cryptocurrency and DeFi markets¹⁴⁸. The prevalence of concentration, collusion, exploitation, and malfunction risks underscores ongoing vulnerabilities for retail investors, including cybersecurity risks, market manipulation, volatility, liquidity impairment, and significant price fluctuations stemming from the actions of a limited number of entities¹⁴⁹.

- **Challenges and Regulatory Approaches to AML in DeFi**

A decentralized exchange, or "DEX," is a core activity within DeFi that facilitates the exchange of cryptographic assets and enables international transactions without intermediaries. This characteristic can potentially be exploited by money launderers if the DEX lacks a robust compliance system¹⁵⁰. The Financial Action Task Force (FATF), an international body that sets standards for combating money laundering and terrorist financing, has recognized this issue, highlighting anti-money laundering (AML) as a critical concern in DeFi. Implementing AML measures in DeFi is challenging because the system relies heavily on automated application programs, such as smart contracts, which operate without direct human oversight. This automation makes it difficult to monitor and enforce compliance with traditional AML protocols, as there are no centralized authorities to oversee transactions and identify suspicious activities.¹⁵¹ Regardless

¹⁴⁶ Billy Bambrough, "New Research Reveals 'Systemic Risk' To Bitcoin As Its Price Crashes Under \$60,000" (27 October 2021), online: Forbes <www.forbes.com/sites/billybambrough/2021/10/27/new-research-reveals-systemic-risk-to-bitcoin-as-its-price-crashes-under-60000/?sh=51530373e066>.

¹⁴⁷ Olga Kharif, "Bitcoin Whales' Ownership Concentration is Rising During Rally" (18 November 2020), online: BNN Bloomberg <www.bnnbloomberg.ca/bitcoin-whales-ownership-concentration-is-rising-during-rally-1.1524504>.

¹⁴⁸ Raphael Auer, Jon Frost & Jose Maria Vidal Pastor, "Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi" (16 June 2022), online: BIS Bulletin No. 58 <www.bis.org/publ/bisbull58.htm>.

¹⁴⁹ James Angel & Ryosuke Ushida, "Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs" in FC 2021 International Workshops, in Matthew Bernhard et al., eds., *Financial Cryptography and Data Security FC 2021 International Workshops* (Berlin: Springer, 2021) 21 at 33.

¹⁵⁰ Tomonori Yuyama, Ken Katayama & Paul Brigner (2023), see note 75.

¹⁵¹ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Paris: FATF, 2021) at 1, online: FATF <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>.

of the scale of a DeFi platform, it must not be used to fund illegal activities, making AML measures crucial. To combat money laundering, Know Your Client (“KYC”) protocols, such as identity verification, need to be incorporated into DeFi in some capacity¹⁵². In 2021, the FATF proposed draft guidance to broaden the definition of virtual assets service providers (“VASP”) to include any entity developing or operating a DeFi platform, even if they do not directly interact with users.¹⁵³ The challenge remains on how to implement AML countermeasures within DeFi, which is essentially an application program¹⁵⁴. The FATF also indicates that DeFi and stablecoins, despite their regulatory ambiguity, should adhere to the "travel rule." This rule mandates that VASPs collect and share information on the sender and recipient of crypto-asset transactions to prevent money laundering. According to the FATF (2021), almost all DeFi platforms qualify as VASPs¹⁵⁵. The FATF cautions regulators against uncritically accepting the crypto industry's broad use of the term "decentralized" for various platforms, as there is often a person who "controls or influences" the platform's activities. Identifying this point of control or influence is crucial for determining who must comply with AML/CFT regulations. Despite these regulatory challenges, including concerns about privacy, fairness, financial inclusion, and enforceability, the central issue remains how to enforce AML as DeFi continues to evolve¹⁵⁶. Some propose embedding AML protocols directly into the code through systems like AML Oracle (Coinfirm)¹⁵⁷, which aims to execute AML measures automatically via smart contracts. However, this technology is still in its early stages and its practical effectiveness remains uncertain¹⁵⁸. It is argued that even if a DeFi platform does not engage with disclosure platforms or fall under the regulation of financial

¹⁵² Tomonori Yuyama, Ken Katayama & Paul Brigner (2023), see note 75.

¹⁵³ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Paris: FATF, 2021) at 1, online: FATF <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>.

¹⁵⁴ Tomonori Yuyama, Ken Katayama & Paul Brigner (2023), see note 75.

¹⁵⁵ FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Paris: FATF, 2021) at 1, online: FATF <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>.

¹⁵⁶ BGIN, Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations, BGIN SR 001 (2021) at 1.

¹⁵⁷ Coinfirm Releases Smart Contract AML Oracle For DeFi Compliance (5 May 2022), online: Businesswire <https://www.businesswire.com/news/home/20220505006077/en/Coinfirm-Releases-Smart-Contract-AML-Oracle-For-DeFi-Compliance>

¹⁵⁸ Tomonori Yuyama, Ken Katayama & Paul Brigner (2023), see note 75.

services, it should still adhere to AML/CFT and other financial legal measures as outlined by FATF standards, which are designed to be applicable to DeFi¹⁵⁹.

The underlying philosophy and goals of DeFi and Fintech contribute significantly to their disparities. DeFi aims to create a more inclusive and permissionless financial ecosystem, reducing reliance on traditional financial institutions and challenging the need for centralized control. This decentralized nature raises important questions about the feasibility and scope of regulation within DeFi. While DeFi operates outside traditional regulatory frameworks, there is an ongoing debate about how, or if, it can be effectively regulated without undermining its core principles. In contrast, Fintech primarily seeks to enhance existing financial services through technological innovation, operating within established financial structures and regulatory frameworks, albeit subject to ongoing adaptations in response to technological innovations.

In conclusion, the differentiation between DeFi and Fintech emerges from their approaches to decentralization, regulatory frameworks, and overarching objectives within the broader context of financial services. The differentiation between DeFi and Fintech emanates from their fundamental operational and structural characteristics. DeFi operates in a more nascent and dynamically evolving regulatory landscape, often navigating uncertainties as regulatory bodies endeavor to catch up with the rapid advancements in decentralized technologies. The question of whether DeFi can be regulated applying financial legislation remains complex, as any attempt to regulate it must balance the need for oversight with the preservation of its decentralized ethos.

¹⁵⁹ Ibid

Chapter VI: Overview of Canadian Law

In Canada, the regulatory landscape for DeFi remains notably decentralized and lacks specific frameworks tailored to this emerging sector. Unlike traditional finance, where specific regulations often govern various aspects of the industry, DeFi operates in a regulatory environment characterized by a broad application of existing legislative schemes designed for conventional financial systems. As of now, there is no dedicated regulatory framework exclusively addressing the unique challenges and opportunities presented by decentralized financial technologies.

Numerous DeFi protocols and applications currently function in Canada without undergoing registration or regulatory supervision, notably lacking “know your customer” (KYC) screening, anti-money laundering, or counter-terrorist financing prevention measures¹⁶⁰. DeFi applications pose considerable regulatory challenges in Canada due to their operation without traditional intermediaries or custodial services. Instead, they rely on automated, open-source smart contracts or software protocols, enabling global peer-to-peer interactions on decentralized, programmable blockchains accessible through user-controlled wallets.¹⁶¹ The diverse range of potential regulated entities imposes significant enforcement costs and uncertainties¹⁶².

Certain DeFi applications, such as automated peer-to-peer borrowing and lending protocols, and protocols for generating synthetic assets, may implicate securities or derivatives regulations¹⁶³. Similarly, some DeFi prediction markets, based on smart contracts, may resemble binary options, which are prohibited in certain provinces¹⁶⁴. Others may resemble illegal lotteries, betting pools, or prediction markets¹⁶⁵. Automated DeFi exchanges may also serve a marketplace function akin to Crypto-Trading Platforms (“CTPs”) covered by CSA Staff Notice 21-327, despite

¹⁶⁰ Ryan Clements (2021), See note 90

¹⁶¹ Ibid; Lewis Cohen, Angela Angelovska-Wilson & Greg Strong, "Decentralized Finance: Have Digital Assets and Open Blockchain Networks Found Their 'Killer App'?" (2021) Global Legal Insights, Blockchain & Cryptocurrency Regulation.

¹⁶² Ryan Clements & Virginia Torrie (2023), see note 128

¹⁶³ Johannes R. Jensen, Victor von Wachter & Omri Ross, "An Introduction to Decentralized Finance (DeFi)" (2021) 26 *Complex Systems Informatic & Modeling Q.* 46 at 50-51.

¹⁶⁴ Ontario Securities Commission, CSA Multilateral Notice of Multilateral Instrument 91-102, Prohibition of Binary Options and Related Companion Policy (28 September 2017), online: OSC <www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170927_91-102_binaryoptions.htm>.

¹⁶⁵ Ryan Clements (2021), See note 90

lacking investor protections such as disclosures, platform-level operational integrity, internal controls, or protocol registration¹⁶⁶. Even with the establishment of regulatory policies, enforcing regulations in the DeFi sphere will prove challenging¹⁶⁷ and may necessitate measures such as blocking orders against non-compliant websites, a remedy previously utilized in Canada in the context of copyright infringement¹⁶⁸.

The Joint CSA-IIROC Staff Notice 21-329, issued by the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC), provides guidance on the regulation of cryptocurrency trading platforms. This notice primarily focuses on the regulatory expectations for platforms that facilitate the buying, selling, and custody of crypto assets. However, it does not offer specific guidance on intermediated DeFi services, such as crypto-staking, cryptocurrency deposits, liquidity transformation, DeFi yield farming, or crypto-lending, leaving these areas without clear regulatory direction.¹⁶⁹

These intermediated DeFi and lending services have the potential to introduce novel securities or derivatives, adopting characteristics akin to "evidence of indebtedness" based securities or "investment contracts," and they may also resemble traditional deposits¹⁷⁰. For instance, in the context of staking, a crypto-asset is pledged ("staked") to earn rewards, thereby facilitating a consensus mechanism on a proof-of-stake ("PoS") blockchain network and contributing to the network's stable operations. The U.S. Securities and Exchange Commission (SEC) has asserted that intermediated "staking-as-a-service" activities carried out by CTPs on behalf of their clients constitute securities, meaning that these activities fall under the purview of securities regulations. Consequently, the SEC has actively pursued enforcement measures against

¹⁶⁶ Canadian Securities Administrators, CSA Staff Notice 21-327, Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets (16 January 2020)

¹⁶⁷ David Gogel et al., "DeFi Beyond the Hype: The Emerging World of Decentralized Finance," Wharton Blockchain & Digital Asset Project, Wharton School, University of Pennsylvania (2021), online (pdf): WIFPR <wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf>.

¹⁶⁸ *Teksavvy Solutions Inc. v. Bell Media Inc.*, 2021 CAF 100, 2021 FCA 100, 2021 CarswellNat 1539, 2021 CarswellNat 7319, [2021] 4 F.C.R. 112, 460 D.L.R. (4th) 136 (F.C.A.); additional reasons 2021 CAF 181, 2021 FCA 181, 2021 CarswellNat 3930, 2021 CarswellNat 8219 (F.C.A.); leave to appeal refused 2022 CarswellNat 716, 2022 CarswellNat 717 (S.C.C.).

¹⁶⁹ Ryan Clements & Virginia Torrie (August 2023), pp. 345-380, see note 128.

¹⁷⁰ Ryan Clements (2021), See note 90

prominent CTPs like Kraken and Coinbase, viewing intermediated staking as an unlawful offering of securities¹⁷¹. In Canada, CTPs intending to provide intermediated staking services must obtain prior consent from their principal regulator as part of pre-registration requirements¹⁷². Initially, the Canadian Securities Administrators (CSA) granted approvals for intermediated staking to several crypto trading platforms (CTPs). However, the collapse of FTX, following its bankruptcy and allegations of fraud, has significantly hindered progress in this domain.

The absence of specific DeFi regulations in Canada has led to a situation where a diverse range of legislative measures originally intended for traditional financial institutions are applied to the cryptocurrency and blockchain space. This includes regulations pertaining to securities, AML, and KYC compliance requirements, among others. While this approach offers a degree of regulatory oversight, it also highlights the adaptability of existing laws to encompass the dynamic and evolving nature of DeFi.

However, it's crucial to note that the federal regulatory environment in Canada, while prudential, is not directly responsible for securities regulation or secured lending, as these are primarily under provincial jurisdiction. The federal government is implicated in areas where it has constitutional authority, such as criminal law and bankruptcy, but its role in regulating DeFi is less clear-cut. This implies that while a regulatory framework exists, its application and enforcement may not be straightforward or comprehensive when applied to decentralized financial platforms. This regulatory uncertainty underscores the need for ongoing discussions and potential future developments in Canadian legislation to more precisely address the nuances of DeFi and ensure a balanced regulatory approach that fosters innovation while safeguarding market participants.

The absence of a standardized legal definition for virtual assets and currencies poses challenges in regulatory efforts. There is a pressing need for lawmakers to precisely define these

¹⁷¹ U.S. Securities and Exchange Commission, Press Release, "Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay \$30 Million to Settle SEC Charges" (9 February 2023), online: SEC <www.sec.gov/news/press-release/2023-25>.

¹⁷² Claire Brownell, "With Crypto-Staking Approvals, Canada's Securities Regulators Mark Another World First" (17 November 2022), online: The Logic <thelogic.co/news/with-crypto-staking-approvals-canadas-securities-regulators-mark-another-worldfirst/>.

terms to avoid ambiguity and ensure consistency in regulatory application. Tokenization can yield a wide array of outcomes. Over the past year, analysts have delineated three classifications based on the presence or absence of specific features: currency tokens, utility tokens, and investment tokens¹⁷³. Given the capacity to imbue tokens with various attributes, hybrid tokens may arise, posing considerable challenges for existing regulatory frameworks.¹⁷⁴ When it comes to classification of tokens, it is crucial to consider the rapidly evolving nature of the digital asset space, as rigid definitions based solely on current classifications might not be future-proof. Therefore, it may be more effective for lawmakers to adopt a flexible, principles-based approach, allowing for adaptability as the technology and market evolve. It is also worth noting that the regulation of virtual assets in Canada would likely fall under provincial jurisdiction rather than federal. This necessitates a tailored approach to regulation within the Canadian context, taking into account the constitutional division of powers and the need for provincial legislation that reflects the unique aspects of each province's financial and legal environment.

Such definitions should account for the diverse nature of tokens within the cryptocurrency space, considering factors such as utility, security, or investment characteristics. Furthermore, to enhance regulatory efficacy, a tiered approach may be warranted. This involves categorizing tokens based on their classification and nature, leading to the assignment of specific supervisory authorities for oversight. Tailoring regulatory oversight to the unique characteristics of each token type acknowledges the nuanced risks and functionalities associated with different decentralized financial instruments. In essence, a clear legal framework and well-defined categories for virtual assets, currencies, and tokens, coupled with specialized supervisory authorities, are essential

¹⁷³ Lars Klöhn et al., "Initial Coin Offerings (ICOs)," 30, *Zeitschrift für Bankrecht und Bankwirtschaft* 89, 99 (2018); Iris M. Barsan, "Legal Challenges of Initial Coin Offerings," 2017 *Revue Trimestrielle de Droit Financier* 54, 56-60; Jonathan Rohr & Aaron Wright, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets" (U. Tenn. Legal Stud. Res. Paper No. 338, *Cardozo Legal Stud. Res. Paper No. 527*, 2018), at 14–26, available at https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=3845&context=hastings_law_journal.

¹⁷⁴ Philipp Hacker & Chris Thomale, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law" (last revised May 2, 2018), 33–37, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820.

components for building a regulatory infrastructure capable of fostering innovation while safeguarding against potential risks in the rapidly evolving DeFi and cryptocurrency ecosystem.

The classification of virtual tokens into utility tokens, payment tokens, security tokens, tokens issued by decentralized autonomous organizations, and cryptocurrencies, is instrumental in shaping effective DeFi regulation and ensuring robust investor protection. This categorization establishes a structured framework that addresses the diverse functions and characteristics of digital assets, offering clarity to regulators, market participants, and investors alike.

- Bitcoin (BTC) is classified as a cryptocurrency, and its decentralized nature means it is often considered outside traditional regulatory frameworks. Cryptocurrencies, as a broad category, play a role in enabling cross-border transactions. Their decentralized and borderless nature¹⁷⁵ underscore the importance of recognizing them as a distinct asset class for regulatory purposes, allowing for the facilitation of global financial activities. Thanks to their predominantly decentralized nature, cryptocurrencies often do not entail an ongoing association with an issuer¹⁷⁶, a characteristic pivotal to investment and utility tokens. Like the majority of these cryptocurrencies, Bitcoin stems from open-source initiatives, thus lacking a central governing entity. They facilitate transactions as a means of payment, usable in exchanges with any party consenting to accept them¹⁷⁷. The confidence vested by market participants in currency tokens doesn't derive from the support of a central bank but rather from the inherent security of the blockchain technology, which is highly resistant to manipulation¹⁷⁸.
- Utility Tokens, such as those used for accessing a decentralized application, carry different risks compared to Security Tokens, which represent ownership in an asset. For example,

¹⁷⁵ Bitcoin, Monero, and Verge serve as illustrations of decentralized cryptocurrencies.

¹⁷⁶ Philipp Maume & Mathias Fromberger, "Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws," (2019) 19.2 Chicago Journal of International Law (accessed on May 8, 2024), available at <https://cjlil.uchicago.edu/print-archive/regulation-initial-coin-offerings-reconciling-us-and-eu-securities-laws>.

¹⁷⁷ Ibid.

¹⁷⁸ Iris M. Barsan, "Legal Challenges of Initial Coin Offerings," 2017 Revue Trimestrielle de Droit Financier 54, at p. 57.

the Basic Attention Token (BAT)¹⁷⁹ is a utility token that provides access to services within the Brave browser ecosystem, enabling users to earn tokens by viewing privacy-respecting ads. Another example is the Chainlink (LINK) token,¹⁸⁰ which is used to pay for services within the Chainlink decentralized oracle network, connecting smart contracts to real-world data. These utility tokens enable specific functionalities within their respective platforms, distinguishing them from security tokens, which are tied to ownership or investment in assets. For instance, utility tokens like BAT and LINK are tied to the operational aspects of their platforms, meaning that their value and associated risks are linked to the performance and adoption of those platforms. In contrast, security tokens, which represent ownership in assets or shares, carry risks associated with the underlying asset or the issuing company's performance. For utility tokens, the focus might be on ensuring that the token's functionality is transparent and that users are protected from misleading claims about the token's utility. This ensures a fair and transparent market environment for all participants. Ethereum-based ERC-20 tokens, like Uniswap's governance token UNI, fall under the Utility Token category. Regulatory compliance is maintained through transparent utility functionalities, ensuring that users and investors can clearly understand the token's purpose and associated risks.

- Security Tokens are subject to stringent securities regulations, including disclosure requirements. Proper classification enables investors to understand the specific risks associated with each type of token and helps prevent fraudulent activities and market manipulation by ensuring that issuers adhere to transparent practices, ultimately safeguarding investors and fostering informed decision-making. A detailed analysis of how securities laws apply to tokens, will be covered in the upcoming chapters.
- Tokens issued by Decentralised Autonomous Organisations are associated with decentralized governance structures, providing token holders with decision-making

¹⁷⁹ Basic Attention Token, online: <https://basicattentiontoken.org/>.

¹⁸⁰ Chainlink, "*LINK Token Contracts*", online: <https://docs.chain.link/resources/link-token-contracts>.

powers¹⁸¹. In the DAO, the funds raised were designated for financing additional projects, with the aim of generating returns for DAO token subscribers. While DAO tokens provide voting rights and potential returns, they may not necessarily qualify as securities, as they might not meet the specific legal definition of an investment contract,¹⁸² as DAOs can be used for many different reasons (ie. community-focused DAOs, knowledge-sharing cooperatives), and its value is primarily driven by the collective actions of its DAO community rather than the efforts of a central management team.¹⁸³ A cohort involved in issuing the DAO tokens, known as the "Curators," would identify suitable projects in advance. Subsequently, token subscribers would have the opportunity to vote on which of these projects should receive funding¹⁸⁴. Classifying tokens as DAO Tokens clarifies the governance rights of participants, reducing ambiguity and enhancing transparency in decentralized organizations.

- Tokens designed for facilitating transactions, such as Ripple's XRP, are categorized as Payment Tokens. Unlike decentralized currency tokens like Bitcoin, which function as a store of value or medium of exchange, Payment Tokens are often more centralized and specifically tailored for use in digital payments. This alignment with payment regulations ensures that users engaging in transactions with these tokens benefit from regulatory safeguards, promoting trust in their payment functionalities.

Some scholars argue that currency tokens are typically characterized as decentralized and lacking intrinsic value¹⁸⁵. However, if a currency token integrates payment functionalities with investment features beyond mere value appreciation, it may still serve as a payment instrument, but its primary classification would shift to that of an investment token. This reclassification

¹⁸¹ Vitalik Buterin, "A Next Generation Smart Contract & Decentralized Application Platform," Ethereum White Paper (2013)

¹⁸² See The Supreme Court of Canada's decision in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 S.C.R. 112

¹⁸³ *Ibid*

¹⁸⁴ Philipp Maume & Mathias Fromberger (2019), see note 175

¹⁸⁵ Hermann Treiblmaier, "Do Cryptocurrencies Really Have (No) Intrinsic Value?" (2022) 32 *Electron Markets* 1749 at 1758, online: <https://doi.org/10.1007/s12525-021-00491-2>.

emphasizes its dual role, where the token now functions not only as a medium of exchange but also as an investment vehicle.¹⁸⁶

- Stablecoins.

Stablecoins represent a distinct class of digital assets within the cryptocurrency landscape. Unlike the inherent volatility commonly associated with traditional cryptocurrencies such as Bitcoin, stablecoins are specifically designed to maintain a stable value, often pegged to traditional fiat currencies like the US Dollar, or other assets such as commodities or baskets of currencies. The primary objective of stablecoins is to mitigate the price volatility that can be a significant characteristic of other cryptocurrencies¹⁸⁷. This stability is typically achieved through pegging mechanisms, collateralization, or algorithms. Pegged stablecoins maintain a fixed value in relation to a chosen asset, ensuring a consistent exchange rate. Collateralized stablecoins, on the other hand, are backed by reserves of assets, providing a degree of stability through the backing of real-world value¹⁸⁸. Algorithmic stablecoins utilize algorithms and smart contracts to dynamically adjust the supply to maintain a stable value.

From a regulatory perspective, stablecoins raise various considerations. The pegging of stablecoins to fiat currencies may prompt inquiries into the regulatory status of these digital assets, potentially subjecting them to existing financial regulations. Additionally, the collateralization of stablecoins requires scrutiny to ensure the adequacy and transparency of the underlying reserves. Smart contracts play a crucial role in many stablecoin systems, automating functions such as issuance, redemption, and governance. In their staff analytical note,¹⁸⁹ the Bank of Canada refers to stablecoins as “fiat-referenced crypto assets”. The creation of fiat-referenced cryptoassets involves both on-chain and off-chain activities. On-chain, the issuer selects the blockchain,

¹⁸⁶ Ibid

¹⁸⁷ Klaudia Jarno & Hanna Kołodziejczyk, "Does the Design of Stablecoins Impact Their Volatility?" (2021) 14(2) *Journal of Risk Financial Management* 42, online: <https://doi.org/10.3390/jrfm14020042>.

¹⁸⁸ Roman Kozhan & Ganesh Viswanath-Natraj, "Decentralized Stablecoins and Collateral Risk" (1 September 2021), online (pdf): https://acfr.aut.ac.nz/_data/assets/pdf_file/0004/570307/DAI_Paper_SSRNSeptember2021.pdf.

¹⁸⁹ Bank of Canada, "Potential benefits and key risks of fiat-referenced cryptoassets," Staff Analytical Note 2022-20, by Hugh Ding, Natasha Khan, Bena Lands, Cameron MacDonald, Laura Zhao, December 2022, <https://www.bankofcanada.ca/2022/12/staff-analytical-note-2022-20/>.

develops the code for token creation, and manages token supply. Off-chain, the issuer sets investment policies for reserve assets and often engages third parties, such as asset managers and custodians, to handle reserve management. The issuer thus acts as a bridge between the cryptoasset ecosystem and the traditional financial system¹⁹⁰.

Distribution of fiat-referenced cryptoassets typically does not occur directly to the public; instead, issuers collaborate with intermediaries like cryptoasset trading platforms and custodial wallets. Intermediaries acquire large amounts of these assets for distribution to end-users. End-users commonly interact with these tokens through intermediaries, who offer custody services and settle off-chain transactions on their own ledgers, often more cost-effectively than on the blockchain.

Presently, stablecoins play a prominent role as the medium of exchange and store of value on numerous centralized crypto exchanges and DeFi platforms. Utilizing these assets within the crypto ecosystem, as opposed to fiat currency, offers several potential advantages, including the facilitation of DLT-based financial services. Furthermore, it is likely more cost-effective and operationally efficient for exchanges to manage liquidity using fiat-referenced cryptoassets instead of fiat currency. This is attributed to the following factors:

- Cryptocurrency blockchain transactions can settle at a quicker pace compared to transactions involving traditional fiat currency.
- Blockchains operate continuously, whereas many fiat payment systems are constrained by typical banking business hours.
- Certain exchanges may lack the necessary banking relationships to support specific fiat currencies.

Beyond their current role in the crypto ecosystem, stablecoins may see broader adoption as a medium of payment for everyday transactions and peer-to-peer dealings. This potential expansion

¹⁹⁰ Ibid

could position these cryptoassets as significant players in the future financial system¹⁹¹. Their utility extends to "smart contracts," enabling automated payments based on predefined conditions, aligning with the concept of "programmable money"¹⁹². Examples include fund transfers for a house purchase upon receipt and confirmation of an inspection report or funds designated for specific purchases with expiration after a stipulated time¹⁹³. Integration of fiat-referenced cryptoassets in smart contracts also supports micropayments, including autonomous machine-to-machine transactions, where computers can remunerate each other for processing power or file storage space. Furthermore, proponents argue that these assets have the potential to advance financial inclusion, theoretically being accessible to anyone, although current costs may pose barriers¹⁹⁴.

However, there is a belief among EU experts that crypto-assets, deriving their value from traditional financial instruments such as currency or securities and commonly referred to as "stablecoins", have the potential to introduce systemic risks, particularly in the form of currency risk. The adoption of these assets, especially on a large scale, could pose challenges to both financial and monetary policies, depending on the specifics of their pegging arrangements. It is essential for users to have the capability to redeem the crypto asset into the underlying fiat currencies or other assets to which it is pegged. However, jurisdictions vary in terms of currency constraints and foreign exchange management practices, making it unclear how these redemptions will operate. Additionally, the influence of each stablecoin on the foreign exchange reserves of the countries where users hold them is a significant consideration. Less economically developed nations often lack substantial foreign exchange reserves and may impose restrictions on the acquisition of foreign currencies. Consequently, the functioning of convertibility in such

¹⁹¹ Christian Catalini & Jai Massari, "Stablecoins and the Future of Money," Harvard Business Review (August 10, 2021), <https://hbr.org/2021/08/stablecoins-and-the-future-of-money>.

¹⁹² Alex Lipton, Stuart Levi, Skadden, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations," Harvard Law School Forum on Corporate Governance (May 26, 2018)

¹⁹³ Douglas Arner, Raphael Auer, and Jon Frost, "Stablecoins: Risks, Potential and Regulation," Bank for International Settlements Working Paper No. 905

¹⁹⁴ Bank of Canada (2022), see note 189

jurisdictions is ambiguous, and the potential downstream implications for the financial system are uncertain.¹⁹⁵

The Bank of Canada in its staff analytical note¹⁹⁶ argues that inadequate regulation and disclosure in the realm of fiat-referenced crypto assets may expose consumers and investors to an elevated risk of encountering fraud or falling victim to investment scams. The absence of consumer protection and market conduct regulations leaves holders uninformed about their rights and obligations. Additionally, the Bank of Canada claims that consumers and investors may be misled into perceiving these crypto assets as entirely risk-free. The use of the term "stablecoins" may contribute to this misconception, creating the impression that the price will remain pegged without deviation, both in typical market conditions and during stressful events. Assertions about these crypto assets being backed by reserve assets may further mislead holders into believing they possess a secure claim on reserves without any redemption restrictions. The widespread adoption of fiat-referenced crypto assets could consequently pose risks with potential implications for financial stability.

There are opinions suggesting that while many cryptocurrencies exhibit high volatility and illiquidity, including some that are marketed as stablecoins, they are often promoted as secure and suitable investments. This raises concerns about deceptive practices and insufficient disclosures. For instance, stablecoins are generally designed to maintain a stable value by being pegged to a fiat currency or other assets, but the underlying collateral or market conditions can still lead to fluctuations, especially if there are doubts about the issuer's solvency or the collateral's liquidity.¹⁹⁷ Simply disseminating standard disclaimers to consumers and institutional investors may not adequately address these issues. Cybersecurity concerns persist, with instances of cryptocurrency theft from online wallets and cases where creators or sponsors of a cryptocurrency disappeared

¹⁹⁵ Expert Group on Regulatory Obstacles to Financial Innovation (2019), see note 14. at p.57

¹⁹⁶ Bank of Canada (2022), see note 189.

¹⁹⁷ Christian Catalini & Alonso de Gortari, "On the Economic Design of Stablecoins" (5 August 2021), online: SSRN <https://ssrn.com/abstract=3899499>.

with substantial amounts of that particular class of cryptocurrency¹⁹⁸. European Central Bank President Draghi emphasized during a September 2017 press conference that no Eurozone member state can introduce its own digital currency, reaffirming the Euro as the sole legal tender in the Eurozone. In 2020, the International Monetary Fund found that fewer than forty-five countries have laws permitting the issuance of government-backed cryptocurrencies under existing banking, financial, and other regulations. The prevailing hype around cryptocurrencies may be unwarranted and potentially criminal activity because official national currencies are already digitally transacted, represented, and accepted as "digital equivalents" in the digital/virtual economy¹⁹⁹.

Stablecoins present numerous risks, with the nature of these risks being contingent upon the stablecoin's design and the operational practices of its issuer²⁰⁰. For instance, uncollateralized algorithmic stablecoins like UST, which experienced significant failure in May 2022, possess distinct dependencies on external market actors and ongoing demand within a correlated cryptocurrency (such as LUNA in the case of UST) to ensure operational stability²⁰¹. In contrast, off-chain "fiat-backed" stablecoins, which maintain reserves of liquid assets to uphold a pegged value, introduce three broad categories of risk: consumer and investor protection concerns, micro-prudential risks at the firm level of the stablecoin issuer, and macro-prudential risks affecting the broader financial system²⁰².

First, consumers and investors of stablecoins face significant risks related to data privacy, cybersecurity, and transparency.²⁰³ For instance, if a stablecoin issuer fails to adequately secure its platform, a breach could expose sensitive user data or even result in the loss of funds, as seen in the case of certain centralized exchanges. Additionally, without clear transparency on reserve

¹⁹⁸ Harvey et al. (2021), See note 34.

¹⁹⁹ Ibid

²⁰⁰ Ryan Clements, "Built to Fail: The Inherent Fragility of Algorithmic Stablecoins" (2021) 11 Wake Forest L. Rev. Online 131, online: Wake Forest Law Review <www.wakeforestlawreview.com/2021/10/built-to-fail-the-inherent-fragility-of-algorithmic-stablecoins/> p. 134-137

²⁰¹ Ibid. at 139-144.

²⁰² Ryan Clements, "Defining the Regulatory Perimeter for Stablecoins in Canada" (2022) 66 Can. Bus. L. J. 201 at 12.

²⁰³ Ibid. at 5-12.

composition and operational practices, investors may not be fully informed about the stability or liquidity of the assets backing their stablecoins, leading to a potential mismatch in perceived versus actual risk.

Second, at the firm level, stablecoin issuers confront micro-prudential risks that can threaten their operational stability. For example, if the custodian holding the reserves were to become insolvent, this could jeopardize the ability of the stablecoin issuer to redeem tokens at their pegged value, leading to potential losses for investors²⁰⁴. Robust internal risk management controls and governance mechanisms are necessary to mitigate these risks, but they may not always be sufficient to fully protect against operational failures or cybersecurity threats²⁰⁵.

Finally, stablecoins introduce macro-prudential systemic risks, particularly when they are widely used as a means of payment. One significant risk is the potential for systemic contagion in the event of a "run" on a stablecoin, where a sudden loss of confidence could lead to mass redemptions, forcing the issuer to liquidate assets at fire-sale prices. This scenario could have ripple effects across the financial system, particularly if the stablecoin is heavily integrated into payment systems or financial markets, similar to the risks posed by shadow banking. Additionally, the scalability challenges of underlying blockchain networks, which serve as critical financial market infrastructures, could exacerbate these systemic risks, particularly during periods of high transaction volume. While the requirement for stablecoin issuers to maintain liquid reserves is intended to mitigate some of these risks, such as ensuring redemption at par value, other risks—such as legal risks, operational challenges, and systemic impacts—may not be fully addressed by reserve requirements alone.²⁰⁶ For example, in a situation where a stablecoin issuer faces legal

²⁰⁴ G7 Working Group on Stablecoins, "Investing the Impact of Global Stablecoins" Bank for International Settlements, Committee on Payments and Market Infrastructures (October 2019), online (pdf): BIS <www.bis.org/cpmi/publ/d187.pdf> at 10 [hereinafter G7 Working Group Report].

²⁰⁵ Ryan Clements & Virginia Torrie (2023), see note 128

²⁰⁶ Ryan Clements (2022). p. 14-15, See note 212

action or insolvency, investors might find themselves acting as unsecured creditors, potentially leading to significant financial losses if the reserves are insufficient to cover all claims.

Effectively regulating stablecoins in Canada necessitates inter-agency collaboration, tiered regulatory frameworks, and the development of a taxonomy to delineate contextual parameters for various stablecoin forms across the financial regulatory landscape. Additionally, such regulation must prioritize international cooperation, harmonization efforts, and data-sharing initiatives, given the interconnectedness and potential systemic impact of a global stablecoin issuer's failure²⁰⁷.

- **Analysis of Bill C-249 (44-1): “Encouraging the Growth of the Cryptoasset Sector Act.”**

Bill C-249²⁰⁸ was introduced with the intention of establishing a regulatory framework to foster the growth of the cryptocurrency sector within Canada. The bill, titled the “Encouraging the Growth of the Cryptoasset Sector Act,” advocated for collaboration between the Minister of Finance and industry experts to develop a framework aimed at enhancing innovation in the cryptocurrency space. It also required the finance minister to report on the framework and introduce corresponding legislation within three years of the bill's passage. The proposed legislation recognized the significant economic and innovative potential of crypto assets for Canada, emphasizing the need to lower barriers to entry into the sector while ensuring protection for participants and minimizing administrative burdens. However, the bill was defeated in the House of Commons, with a vote of 199 to 119 against its advancement. The defeat at the second reading means the bill will not proceed for further study or debate²⁰⁹. This outcome not only reflects the challenges inherent in passing private members' bills but also suggests that encouraging the growth of the crypto asset sector may not be a priority shared by Parliament as a whole. The

²⁰⁷ Ibid

²⁰⁸ Bill C-249 (44-1), An Act respecting the encouragement of the growth of the crypto asset sector, Parliament of Canada, <https://www.parl.ca/legisinfo/en/bill/44-1/c-249>

²⁰⁹ Rachel Aiello, "Conservative MP's Bill to Encourage Growth in Cryptocurrency Sector Defeated," CTV News (November 23, 2022), <https://www.ctvnews.ca/politics/conservative-mp-s-bill-to-encourage-growth-in-cryptocurrency-sector-defeated-1.6165880>.

defeat illustrates the ongoing uncertainty and lack of consensus regarding the regulation of this emerging industry.

Canada lacks a comprehensive regulatory structure governing crypto-assets. However, various federal and provincial regulators have implemented governance measures for different segments, use cases, forms, activities, and intermediaries within the crypto-asset industry²¹⁰. While crypto-assets such as Bitcoin and stablecoins are occasionally used for payments, they are not recognized as legal tender in Canada, similar to foreign currencies like US dollars or Euros. The distinction matters because, unlike legal tender, there is no obligation for businesses or individuals to accept crypto-assets as payment, which can limit their broader adoption and use in everyday transactions.

The forthcoming discourse aims to shed light on the classification of tokens, providing an in-depth analysis of their treatment within existing Canadian legal frameworks. An analysis of the disparate methodologies employed by various nations globally in addressing these tokens will also be conducted. Importantly, the thesis will scrutinize regulatory challenges in applying Securities Law in the context of DeFi, the regulatory landscape governing Virtual Asset Service Providers (VASPs), and Decentralised exchanges, and investigate prevalent best practices within this realm. The discussions will pivot towards the formulation of policy recommendations designed to strengthen regulatory frameworks and promote a balanced and innovative environment within the decentralized finance domain.

²¹⁰ Ibid

Chapter VII: Understanding the Regulatory Hurdles for DeFi: Securities Law in a Decentralized World.

Applying traditional regulatory strategies to a new technological ecosystem has been conceptually challenging due to a policy trilemma, known as the innovation trilemma, which complicates the introduction of regulations for innovative services and products²¹¹. Securities regulation faces inherent challenges in effectively regulating DeFi. Firstly, the decentralized and global nature of DeFi platforms complicates regulatory oversight, as their lack of a central authority makes it difficult to determine who should be held accountable. Unlike traditional multinational corporations, which have identifiable entities and governance structures, DeFi platforms operate across borders without a clear jurisdiction, making comprehensive regulatory control challenging. Moreover, cryptocurrencies and many DeFi assets often do not neatly fit into the existing definitions of securities. They are commonly viewed as commodities rather than traditional securities due to their decentralized and open-source nature. The decentralized nature of DeFi platforms, governed by smart contracts and lacking a central authority, blurs the line between what might traditionally be considered a security and what might be viewed as a commodity. This distinction arises because some DeFi assets function more like commodities, lacking the characteristics typically associated with securities, such as profit expectations from the efforts of a central entity.²¹² Furthermore, the absence of well-established theories of liability in digital currency markets presents a challenge for securities regulation. The traditional legal frameworks for securities often lack the adaptability required to address the specific nuances and complexities of the decentralized and rapidly evolving DeFi landscape.

The innovative and rapidly evolving nature of DeFi, along with the unique characteristics of cryptocurrencies, poses challenges for securities regulation to effectively oversee these assets. Some scholars argue that DeFi and Distributed Ledger Technology (“DLT”) may not alter the fundamental risks but could provide novel methods for overseeing these risks. Therefore, rather

²¹¹ Tomonori Yuyama, Ken Katayama & Paul Brigner (2023), see note 75.

²¹² Raphael Anton Auer (2022), see note 87

than trying to adapt DeFi and crypto assets to pre-existing regulations like securities laws, which were created before DLT existed, it is important to consider how these new technologies can be leveraged to enhance risk monitoring in financial markets²¹³.

The most extensive regulatory standards for crypto-assets presently lie within the domain of securities regulation, which is under provincial jurisdiction in Canada. This regulation is governed by statutory authority provided by provincial securities acts and unified regulations coordinated by the Canadian Securities Administrators²¹⁴. There are, however, jurisdictional limits to the application of securities regulation on crypto-assets, which hinge on whether they qualify as a "security" or a "derivative."²¹⁵ Assessing whether a specific crypto-asset falls under the categories of "security" or "derivative," or if a CTP or any related business deals in or offers advice on such assets, involves a nuanced contextual examination that can pose considerable challenges.²¹⁶

The Canadian Securities Administrators ("CSA") released CSA Staff Notice 46-307²¹⁷, Cryptocurrency Offerings, which details the application of securities laws to various cryptocurrency activities such as initial coin offerings ("ICOs"), initial token offerings ("ITOs"), cryptocurrency investment funds, and related trading on cryptocurrency exchanges. This notice provides guidance relevant to Fintech companies, investors, and advisors, addressing the potential applicability of Canadian securities laws to ICOs, ITOs, cryptocurrency exchanges, and investment funds. It follows a press release by the Ontario Securities Commission confirming that Ontario securities laws may apply to the use of DLTs, like blockchain, in financial products or

²¹³ Ibid

²¹⁴ See Canadian Securities Administrators, online: Canadian Securities Administrators <www.securities-administrators.ca/>; Ryan Clements & Virginia Torrie (2023) see note 128.

²¹⁵ Ryan Clements (2021), See note 90, at 27.

²¹⁶ Canadian Securities Administrators, CSA Staff Notice 46-307, Cryptocurrency Offerings (24 August 2017), online (pdf): Canadian Securities Administrators <www.securities-administrators.ca/uploadedFiles/Industry_Resources/2017aout24-46-307avis-acvm-en.pdf> [CSA Staff Notice 46-307]; Canadian Securities Administrators, CSA Staff Notice 46-308, Securities Law Implications for Offerings of Tokens (11 June 2018), online (pdf): Canadian Securities Administrators <www.securities-administrators.ca/uploadedFiles/Industry_Resources/2018juin11-46-308-avis-acvm-en.pdf> [CSA Staff Notice 46-308].

²¹⁷ Ibid, CSA Staff Notice 46-307 Cryptocurrency Offerings;

services²¹⁸. The CSA Notice clarifies that regardless of the terminology used (coin/token instead of share, stock, or equity), such instruments may still fall under the definition of a "security" according to Canadian securities laws. It underscores that advertising a coin or token as a software product does not exempt it from being classified as a security.

The notice highlights the four-prong test to determine if a coin/token is an investment contract,²¹⁹ emphasizing the economic realities of the arrangement. It also discusses the prospectus requirements for offerings to the public, stating that coins/tokens considered securities must comply with prospectus filing or applicable exemptions. Almost all of the exemptions from the prospectus requirement—whether they aim to accommodate small issuers, acknowledge investor sophistication or their ability to bear financial loss, recognize the inherent safety of the securities being sold, or support other rationales—are fundamentally based on a cost-benefit analysis²²⁰. In some cases, the expense of requiring an issuer to prepare a prospectus outweighs the potential benefits, such as enhanced investor protection, that would result from imposing this requirement²²¹. Achieving the right balance between investor protection and capital market efficiency is an extremely challenging but essential task²²². It is sometimes simplistically argued that there can never be too much investor protection²²³. However, this overlooks a basic economic reality: businesses need to be financially viable for the economy to function and for there to be investment opportunities²²⁴. Regulation, unfortunately, is not without cost. It imposes expenses on businesses, which in turn lead to higher consumer prices, lower employee wages, and reduced investor returns²²⁵.

²¹⁸ Ontario Securities Commission, "OSC Highlights Potential Securities Law Requirements for Businesses" (Press Release, 8 March 2017), online: Ontario Securities Commission <https://www.osc.ca/en/news-events/news/osc-highlights-potential-securities-law-requirements-businesses>.

²¹⁹ The Supreme Court of Canada's decision in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 S.C.R. 112;

²²⁰ Christopher C Nicholls, *Securities Law*, 3rd ed (Toronto: Irwin Law Inc, 2023) at 245.

²²¹ *Ibid.*

²²² *Ibid.*

²²³ *Ibid.*

²²⁴ *Ibid.*

²²⁵ *Ibid.*

Regarding cryptocurrency exchanges, the staff notice 46-307 notice mentions regulatory developments in various jurisdictions, including Canada, particularly regarding anti-money laundering and identity verification. Furthermore, the notice addresses dealer registration requirements for businesses involved in ICOs/ITOs, emphasizing factors such as investor solicitation, capital raised, and marketing methods. Platforms trading securities-like tokens may be considered marketplaces and must comply with marketplace requirements. Concerning cryptocurrency investment funds, the notice discusses registration requirements, valuation methods, due diligence, and regulatory compliance for retail investors. The notice concludes by advising businesses planning ICOs, ITOs, or cryptocurrency investment funds to assess whether securities laws apply and to consult their local securities regulatory authority for compliance approaches. It was also noted that some businesses market their coins/tokens as software products, asserting that they fall outside the purview of securities regulations. However, upon comprehensive evaluation of the complete offering or arrangement, these coins/tokens often merit classification as securities. When determining the applicability of securities laws, regulators prioritize the actual substance of the offering rather than its superficial form²²⁶.

Further to the notice mentioned above, on June 11, 2018, CSA released another Staff Notice 46-308 "Securities Law Implications for Offerings of Tokens", providing guidance on the applicability of securities laws to token offerings²²⁷. Staff Notice addresses the application of securities laws to offerings of coins or tokens, particularly focusing on "utility tokens." It emphasizes that many cryptocurrency offerings, including ICOs and ITOs, may involve the sale of securities, as they can be considered investment contracts or securities under various branches of the definition. The notice provides guidance on determining whether an offering of tokens involves securities, highlighting factors such as the investment of money, common enterprise, expectation of profit, and reliance on the efforts of others²²⁸. Furthermore, the notice discusses

²²⁶ CSA Staff Notice 46-307 Cryptocurrency Offerings, See note 216

²²⁷ CSA Staff Notice 46-308, "Securities Law Implications for Offerings of Tokens", See note 216

²²⁸ Pacific Coast Coin Exchange v. Ontario (Securities Commission), [1978] See note 219.

situations that may impact the presence of elements of an investment contract, such as the purpose of the offering, token delivery, capital raising, marketing strategies, management representations, and token characteristics. It also addresses the trading of tokens on cryptoasset trading platforms and warns against using multiple-step transactions to circumvent securities legislation. The notice highlights the regulatory authority's surveillance of coin and token offerings and its intention to take enforcement action against non-compliant businesses.

As outlined in the CSA Staff Notice 46-307 (2017), businesses meeting specific criteria triggering regulatory obligations²²⁹ have the potential to effectively fulfill their know-your-client (KYC) and suitability responsibilities through a comprehensive, automated online system integrating investor safeguards. These protections might involve imposing limits on investment sums and diversification, alongside issuing risk advisories. Entities facilitating ICOs/ITOs of securities-backed coins/tokens, as mentioned in the same notice, must establish robust compliance frameworks, complete with protocols addressing cybersecurity vulnerabilities. Given the escalating frequency, sophistication, and financial impact of cyber threats, cryptocurrency enterprises must prioritize the implementation of robust cybersecurity measures to shield both their operations and their investors.

The Government of Canada website²³⁰ notes that a common deterrent for individuals engaging with the Bitcoin system is the perceived risk associated with security breaches, primarily involving third-party services like exchanges. Security incidents extend to the hacking of private computers containing Bitcoin "wallets," the software used for system interaction. The website further notes that as the Bitcoin community has matured, security standards have consistently

²²⁹ Companies conducting ICOs/ITOs might engage in securities trading for business purposes, commonly known as the "business trigger," which may necessitate dealer registration or an exemption from such registration. Determining whether an activity meets the business trigger is contingent upon specific factual circumstances. To assess whether its offering meets this criterion, a business should evaluate the factors delineated in section 1.3 of the companion policy to National Instrument 31-103 Registration Requirements, Exemptions and Ongoing Registrant Obligations.

²³⁰ Government of Canada, "Cryptocurrency Guide," Canada Revenue Agency, <https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html>.

improved. In the early stages, new markets may attract rogue operators, but over time, these informal actors tend to be replaced by more formal and regulated entities²³¹ .

- **Regulatory Challenges and Gaps in the Oversight of Stablecoins: Securities, Macroprudential Risks, and the Need for Banking-Like Safeguard.**

In the enhanced pre-registration undertaking (“PRU”) staff notice, issued in February 2023, the CSA acknowledged that certain Value-Referenced Crypto Assets (“VRCAs”), also known as stablecoins, may meet the criteria for classification as securities and/or derivatives in various jurisdictions²³². As a result, the CSA imposed heightened regulatory requirements on CTPs regarding the issuance and trading of VRCAs. These requirements include implementing a consent-based listing system, where the CSA mandates evidence of thorough due diligence to address the associated risks of VRCAs. Additionally, CTPs are obligated to ensure that listed VRCAs are "fiat-backed" and fully reserved with highly liquid assets, such as cash and cash equivalents, subject to monthly attestation and annual independent audits made publicly available. Furthermore, VRCAs must not be collateralized with crypto-assets or gold, and uncollateralized algorithmic varieties of VRCAs are prohibited. Any distribution of VRCAs within Canada must comply with applicable securities legislation. Additionally, CTPs are required to segregate reserves and entrust custody to a qualified custodian on behalf of fiat-backed VRCA holders. Clear and publicly disclosed redemption rights, along with accurate public disclosures, governance parameters, and plans for orderly wind-down, are also mandated to support regulatory compliance and ensure investor protection²³³.

While securities regulators possess various tools to address these risks, their effectiveness, particularly in mitigating macro-prudential risks, is constrained²³⁴. Exclusive regulation of stablecoins under securities law may leave certain gaps unaddressed, such as the absence of macroprudential backstops like lender of last resort facilities or deposit insurance for scenarios

²³¹ Brett Scott (2016) See note 61.

²³² CSA Staff Notice 21-332, (2023), See note 140, p. 10-11

²³³ Ibid at p. 9-13

²³⁴ Ibid, p. 24-28

involving mass redemption runs resembling bank runs. In this context, there is an argument that stablecoin issuers may need to be regulated, to some extent, like banks, particularly when their operations resemble traditional banking activities, such as accepting deposits and managing reserves. This would ensure that stablecoins have access to similar safeguards, such as emergency liquidity support and protection for consumers, which are crucial in maintaining financial stability during periods of market stress. Other overlooked areas include payments-related systemic risks, settlement and clearing risks, challenges associated with global scaling of underlying blockchain networks acting as critical financial market infrastructures, cross-border standardization for global payments, limited consumer protection standards and avenues for recourse for payments-based stablecoins, and inadequacies in AML/CFT measures, and controls against illicit finance²³⁵.

- **Decentralized Exchanges and Virtual Assets Service Providers regulation.**

The rise of DeXs has transformed the way users trade cryptocurrencies. DeXs offer increased security, transparency, and control over funds compared to centralized exchanges, contributing to the growing popularity of DeFi. Effective regulation necessitates identifying a suitable entity to whom rules can be applied and enforced. In the context of virtual currencies like Bitcoin, regulating the individuals controlling the software, referred to here as the “software platform provider”, proves challenging due to their informal and dispersed nature across various jurisdictions. Regulators may explore the option of controlling these networks by compelling local Internet service providers to block relevant data traffic²³⁶. However, this strategy is only partially effective and faces political and legal challenges in democratic settings, especially when less intrusive alternatives are available to regulators. Given these considerations, current regulatory efforts focus on intermediaries situated at the nexus of virtual currencies and the financial market, specifically entities known as virtual currency exchanges—organizations facilitating the exchange of fiat money for virtual currency²³⁷. A similar regulatory approach could be adopted for

²³⁵ Ryan Clements & Torrie, Virginia (2023): p.345-380 see note 127.

²³⁶ Aaron Wright & Primavera De Filippi, see note 8. p.51.

²³⁷ New York Codes, Rules and Regulations, Title 23 Chapter I Part 200 – Virtual Currencies, online: New York Department of Financial Services <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>.

blockchain financial networks that handle securities, fiat money, and derivatives. Nonetheless, it remains uncertain whether this approach would be adequate, especially considering potential risks inherent in blockchain financial networks that might necessitate a holistic regulatory approach²³⁸.

Currently, financial service providers dealing with cryptocurrency transactions in Canada are generally required to register with the Financial Transactions and Reports Analysis Centre of Canada (“FINTRAC”). FINTRAC is the regulatory authority responsible for overseeing compliance with anti-money laundering and counter-terrorist financing regulations in the country. Money Services Businesses (“MSBs”) engaging in cryptocurrency transactions, including exchanges and wallet providers, are subject to these regulations. Registration with FINTRAC involves fulfilling certain reporting and compliance obligations to help prevent illicit financial activities. The potential for illicit activities such as money laundering, drug trafficking, and human trafficking is heightened by the anonymity afforded by cryptocurrencies and their related exchanges. Therefore, it is imperative for such exchanges to consistently verify the identities of participants in the market. Additionally, the disclosure of the executive, founder, and board member identities of crypto-issuers and digital crypto currencies should be made a regular practice.

DeFi platforms commonly function within blockchain networks, presenting a decentralized structure that poses intricate challenges for conventional regulatory frameworks. Frequently lacking a central entity eligible for registration as a MSB, DeFi platforms operate in a decentralized manner, governed by smart contracts. Evaluating the adequacy of MSB registration for DeFi regulation in Canada entails a thorough examination of the distinct activities and structures characterizing DeFi platforms. Several key considerations emerge:

- **Decentralization:** The inherent decentralization of DeFi platforms often means there is no identifiable central entity suitable for MSB registration. This decentralized nature introduces complexities in aligning with established regulatory paradigms.

²³⁸ Philipp Paech (2017), see note 12. p.15

- **Smart Contracts:** DeFi platforms heavily rely on smart contracts to automate financial processes. The regulatory treatment of these smart contracts and their alignment with prevailing financial regulations may necessitate clarification to ensure compliance.
- **Comprehensive Regulatory Approach:** DeFi platforms engage in a spectrum of financial activities extending beyond basic cryptocurrency transactions, including decentralized lending, borrowing, and trading. The regulatory framework must address these diverse functionalities comprehensively to foster effective oversight.

Canadian securities regulators have introduced an innovative and distinctive approach to overseeing crypto-asset trading platforms (also known as crypto exchanges).²³⁹ The establishment of regulatory guidelines for these platforms in Canada was largely prompted by the significant collapse and fraudulent activities associated with Gerald Cotton, the founder of Ontario-based QuadrigaCX, in late 2018²⁴⁰. This incident resulted in the loss of more than \$169 million in customer assets. The failure of QuadrigaCX prompted a public consultation in 2019 by both the CSA and the Investment Industry Regulatory Organization of Canada (IIROC)²⁴¹ to explore the jurisdiction of securities regulation and the potential application of rules for crypto-asset trading platforms²⁴².

In January 2020, the Canadian Securities Administrators (“CSA”) and the Investment Industry Regulatory Organization of Canada (“IIROC”) jointly released guidance (Staff Notice 21-327) outlining the application of securities regulatory frameworks to crypto-asset trading platforms facilitating crypto-assets trading in Canada²⁴³. The guidance specified that the securities

²³⁹ Ryan Clements (2021) See note 89, 27-29.

²⁴⁰ Ontario Securities Commission, "QuadrigaCX: A Review by Staff of the Ontario Securities Commission" (14 April 2020), online: OSC <www.osc.ca/quadrigacxreport/>

²⁴¹ The Investment Industry Regulatory Organization of Canada (IIROC) functions as the nationwide self-regulating body responsible for supervising investment dealers and monitoring trading operations across Canadian equity and debt markets. Recently, IIROC has consolidated with the Mutual Fund Dealers Association, forming the entity known as the "Canadian Investment Regulatory Organization."

²⁴² Canadian Securities Administrators, Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada, Consultation Paper 21-402, Proposed Framework For Crypto-Asset Trading Platforms (14 March 2019), online (PDF): Canadian Securities Administrators <www.securities-administrators.ca/uploadedFiles/Industry_Resources/2019mars14-21-402-doc-cons-en.pdf>

²⁴³ Canadian Securities Administrators, CSA Staff Notice 21-327, Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets (16 January 2020) at 1-2, online: Canadian

regulator would exercise jurisdiction over the trading of crypto assets classified as securities independently. Additionally, regulatory jurisdiction would extend to the trading of crypto-assets classified as commodities (e.g., Bitcoin), even if they were not deemed securities independently, provided that the CTP assumed custody of the commodity crypto-assets and offered users a "contractual right" to delayed, rather than immediate, delivery of the crypto-asset.

This extension of jurisdiction was justified by considering the contractual right to delayed delivery of crypto assets held in custody, as potentially creating a security or derivative, based on the interpretation of relevant definitions such as "investment contract." However, Staff Notice 21-327 provided an exception for certain crypto-asset intermediaries and dealers, exempting them from the application of securities rules if they offered "immediate delivery" of a crypto-asset.

CSA Staff Notice 21-327 was succeeded by CSA / IIROC Staff Notice 21-329, which introduced a nuanced approach to compliance tailored to the operational characteristics of CTPs. This approach involved the implementation of various measures depending on the nature of the CTP's operations. These measures included the establishment of a "restricted dealer" category as a temporary two-year transitional measure before attaining full investment dealer registration, the application of marketplace rules, or a combination of investment dealer and marketplace rules for CTPs undertaking dual functions²⁴⁴. Staff Notice 21-329 identified several significant risks faced by investors engaging with Canadian CTPs. These risks included concerns related to the security of custody arrangements, vulnerabilities in the management of crypto assets (such as private key management), and potential issues with ensuring fair and transparent access to trading platforms. Additionally, there were risks associated with the integrity and robustness of system and security controls, the potential for conflicts of interest, and the challenges of maintaining market integrity

Securities Administrators <www.asc.ca/securities-law-and-policy/regulatory-instruments/21-327> [CSA Staff Notice 21-327]

²⁴⁴ Joint Canadian Securities Administrators / Investment Industry Regulatory Organization of Canada, CSA Staff Notice 21-329, Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements (29 March 2021), online: Canadian Securities Administrators <www.asc.ca/securities-law-and-policy/regulatory-instruments/21327> [CSA Staff Notice 21-329]

Dealer platforms operating in Quebec might also need to undergo registration as derivatives dealers under the Quebec Derivatives Act, C.Q.L.R. c. 1-14.01.

and efficient price discovery. Furthermore, the notice pointed out the importance of strict adherence to know-your-client (“KYC”) and know-your-product (“KYP”) standards as critical components of protecting investors.

Staff Notice 21-329 did not introduce novel regulations for CTPs; instead, it offered guidance on how existing requirements within securities legislation could be customized by applying terms and conditions to the registration or recognition of CTPs, along with discretionary exemptive relief under specific circumstances²⁴⁵. Exemptive relief decisions thus far have encompassed dealer member rules, universal market integrity rules (“UMIR”), and standardized terms and conditions. These conditions include investor limitations and insurance (both third-party and self-insurance), custody regulations, know-your-client (“KYC”) and know-your-product (“KYP”) protocols, and assessing account “appropriateness” akin to suitability standards, particularly for investors with lower risk tolerance levels. Initially, CTPs providing leverage, credit, or margin for crypto-asset trading were confined to a small subset of “permitted clients”²⁴⁶. However, the Alberta Securities Commission (“ASC”) Blanket Order 24-506 imposes restrictions on CTPs, relying on the order for exemption from recognition as a clearing agency, prohibiting them from offering trading margin or leverage to their clients²⁴⁷.

Furthermore, CTPs are obligated to undergo self-certification, confirming the absence of any crypto-assets traded on their platform being classified as “securities” independently²⁴⁸. Additionally, they are mandated to conform to regulations concerning advertising, marketing, and social media promotion²⁴⁹. The Ontario Securities Commission (“OSC”) has taken proactive

²⁴⁵ Ryan Clements (2021), See note 90 at p.32-35

²⁴⁶ See Ontario Securities Commission, “Registered Crypto Asset Trading Platforms,” online: OSC <www.osc.ca/en/industry/registration-and-compliance/registered-crypto-asset-trading-platforms>

²⁴⁷ Alberta Securities Commission, Blanket Order 24-506, Exemption for Certain CTPS to be Recognized as Clearing Agencies (29 August 2022)

²⁴⁸ Ibid

²⁴⁹ Joint Canadian Securities Administrators, Investment Industry Regulatory Organization of Canada, Staff Notice 21-330 - Guidance for Crypto-Trading Platforms: Requirements relating to Advertising, Marketing and Social Media Use (23 September 2021), online: Canadian Securities Administrators <www.asc.ca/securities-law-and-policy/regulatory-instruments/21-330> [hereinafter CSA & IIROC, Staff Notice 21-330].

measures in enforcing actions against CTPs found to be non-compliant²⁵⁰, as well as those involved in market manipulation²⁵¹.

Moreover, in August 2022, the CSA introduced a mandate necessitating CTPs to submit a "pre-registration undertaking to their principal provincial regulator" (referred to as the "Initial PRU"). This undertaking entails a commitment to adhere to terms and conditions aimed at safeguarding investors, akin to the obligations imposed on registered CTPs, during their period of undergoing the IIROC registration process and while their applications are under evaluation²⁵². The Initial PRU was succeeded by an upgraded pre-registration undertaking known as the "Enhanced PRU," introduced by the CSA following Staff Notice 21-332 in February 2023²⁵³. This Enhanced PRU integrated protective measures aimed at averting the issues that led to the collapse of several prominent CTPs in 2022, both in the U.S. and internationally, including Voyager, Celsius, BlockFi, and FTX. The latter case resulted in criminal and civil charges against owner Sam Bankman-Fried and various FTX insiders²⁵⁴. The Enhanced PRU introduced various protective measures, including augmented custody and segregation requirements, which supplemented the initial criteria outlined in the Initial PRU. Moreover, it prohibited the utilization,

²⁵⁰ Ontario Securities Commission, "OSC Holds Global Crypto Asset Trading Platforms Accountable" (22 June 2022), online: OSC <www.osc.ca/en/news-events/news/osc-holds-global-crypto-asset-trading-platforms-accountable>; Ontario Securities Commission, Statement of Allegations, Polo Digital Assets, Ltd (Poloniex), 25 May 2021; Ontario Securities Commission, Statement of Allegations, Mek Global Limited and PhoenixFin Pte Ltd (collectively KuCoin), (2 June 2021); Ontario Securities Commission, Statement of Allegations, Bybit Fintech Limited (Bybit), (21 June 2021) [hereinafter OSC, "OSC Holds Global Crypto Asset Trading Platforms Accountable"; OSC, Statement of Allegations, Polo Digital Assets; OSC, Statement of Allegations, Mek Global Limited and PhoenixFin Pte Ltd; OSC, Statement of Allegations, Bybit Fintech Limited].

²⁵¹ Ontario Securities Commission, In The Matter Of Coinsquare Ltd., Cole Diamond, Virgile Rostand And Felix Mazer, Settlement Agreement (16 July 2020) [hereinafter OSC, Settlement Agreement with Coinsquare Ltd.].

²⁵² Canadian Securities Administrators, "Canadian Securities Regulators Expect Commitments from Crypto Trading Platforms Pursuing Registration" (15 August 2022), online: Canadian Securities Administrators <www.securities-administrators.ca/news/canadian-securities-regulators-expect-commitments-from-crypto-trading-platformspursuing-registration/> [hereinafter CSA, "Canadian Securities Regulators Expect Commitments"].

²⁵³ CSA Staff Notice 21-332, (2023), See note 140

²⁵⁴ U.S. Securities and Exchange Commission, Press Release, "SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX" (13 December 2022), online: SEC <www.sec.gov/news/press-release/2022-219>; United States Department of Justice, Press Release, "United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried" (13 December 2022), online: Department of Justice <www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried>; U.S. Securities and Exchange Commission, Press Release, "SEC Charges Nishad Singh with Defrauding Investors in Crypto Asset Trading Platform FTX" (28 February 2023), online: SEC <www.sec.gov/news/press-release/2023-40>; U.S. Securities and Exchange Commission, Press Release, "SEC Charges Caroline Ellison and Gary Wang with Defrauding Investors in Crypto Asset Trading Platform FTX" (21 December 2022), online: SEC <www.sec.gov/news/press-release/2022-234> [hereinafter SEC Press Releases on FTX Charges].

pledging, or re-hypothecation of client crypto assets, alongside forbidding the provision of margin, credit, or leverage to clients of the CTP. Additionally, a novel stipulation mandated that "controlling mind(s)," including "global affiliates," jointly endorse the Enhanced PRU. The regulations also encompassed restrictions on trading proprietary tokens issued by the CTP or using them for financial calculations. Furthermore, the Enhanced PRU entailed heightened commitments to financial reporting and necessitated the appointment of a Chief Compliance Officer for the CTP. Trading of crypto-contracts linked to crypto-assets classified as securities or derivatives independently was restricted, as well as trading in "Value-Referenced Crypto Assets" (VRCAs), commonly referred to as stablecoins²⁵⁵. The subsequent establishment of pre-registration undertakings, including the Enhanced PRU introduced in February 2023, incorporated additional protective measures to mitigate the recurrence of failures witnessed in high-profile CTPs. These measures included enhanced custody requirements, prohibitions on leveraging, heightened financial reporting commitments, and the imposition of restrictions on trading certain crypto-assets. These stringent requirements signify a proactive approach by regulators to safeguard investor interests and ensure the integrity of the crypto-trading ecosystem.

In conclusion, the regulatory measures implemented by Canadian securities regulators represent a progressive and comprehensive approach towards addressing the challenges posed by CTPs in the evolving landscape of DeFi. By establishing clear regulatory frameworks and enforcing stringent compliance standards, regulators aim to foster investor confidence, mitigate systemic risks, and facilitate the responsible growth of the crypto-trading industry in Canada. Furthermore, transitioning to the next chapter, an examination of DeFi frauds will provide insight into the challenges and vulnerabilities that persist within the decentralized finance ecosystem despite regulatory efforts to enhance oversight and investor protection.

- **DeFi Frauds: Safeguarding Investors in the Crypto Landscape.**

²⁵⁵ CSA Staff Notice 21-332, (2023), See note 139

The cryptocurrency landscape has witnessed a surge in consumer fraud, investment schemes resembling Ponzi schemes, and vulnerabilities for investors²⁵⁶. The Ontario Securities Commission (OSC) has taken decisive enforcement actions against numerous Crypto-Trading Platforms (CTPs) operating without complying with Canadian registration and regulatory requirements, thereby safeguarding Canadian investors²⁵⁷. Moreover, the U.S. Department of Justice recently filed its inaugural indictment against an individual, Nathaniel Chastain, allegedly implicated in an insider-trading scheme involving Non-Fungible Tokens (“NFTs”) on the OpenSea NFT marketplace, which Canadian investors can access²⁵⁸. The Chastain case raises pertinent questions regarding the jurisdiction of securities regulators over NFTs and the classification of NFT transactions as securities, especially as the accused purportedly invested in NFTs with the intention of selling them for profit, rather than acquiring them solely as digital collectibles²⁵⁹. While the Chastain case originates in the United States, its implications resonate in Canada due to similarities in legal interpretations, particularly regarding the expansive definitions of "security" in provincial statutes such as "investment contract."²⁶⁰

Regulators are often challenged with a delicate balancing act atop the high wire of securities regulation, where every step forward holds the promise of innovation and wealth, yet every misstep threatens to plunge investors into the abyss of fraud and deception. This universally recognized dilemma underscores the pivotal role of regulators in navigating the fine line between

²⁵⁶ United States Department of Justice, Office of Public Affairs, "Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving Over \$100 Million in Intended Losses" (30 June 2022), online: Department of Justice <www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud>.

²⁵⁷ Ontario Securities Commission, "OSC Holds Global Crypto Asset Trading Platforms Accountable" (22 June 2022), online: OSC <www.osc.ca/en/news-events/news/oscholds-global-crypto-asset-trading-platforms-accountable>.

²⁵⁸ John Cahill, Jana S. Farmer & William H. Behr, "First DOJ NFT Insider Trading Charges Mark New Enforcement Era" (29 June 2022), online: Bloomberg Law <news.bloomberglaw.com/us-law-week/first-doj-nft-insider-trading-charges-marks-new-enforcement-era-16>.

²⁵⁹ *Ibid.*

²⁶⁰ Securities Act, R.S.O. 1990, c. S.5, s. 1.1 at s.1(a) (security) [OSA]; Securities Act, R.S.A. 2000, c. S-4, s.1 (security) (ggg) [ASA]; Securities Act, R.S.B.C. 1996, c. 418, s.1(1)(security) [BCSA]; *Pacific Coast Coin Exchange of Canada v. Ontario (Securities Commission)*, 1977 CarswellOnt 50; *Ontario Securities Commission, In The Matter Of Coinsquare Ltd., Cole Diamond, Virgile Rostand And Felix Mazer, Settlement Agreement* (16 July 2020); *Re Shelter Corporation of Canada Ltd.*, 1977 O.S.C.B. 6; *Williamson, Re*, 1993 CarswellOnt 1523, 16 O.S.C.B. 2689 (Ont. Securities Comm.); *Jenson v. Continental Financial Corporation*, 404 F.Supp. 792 (D.C. Minn. 4th Div., 1975)

opportunity and risk. As we delve into this complex landscape, each regulatory decision shapes the trajectory between progress and peril, shaping the investment landscape for all stakeholders involved.

Cryptocurrency has garnered extensive recognition due to its decentralized structure, rapid and secure transaction capabilities, and allure for investment and speculative endeavors. However, this surge in popularity has correspondingly resulted in a rise in cryptocurrency-related fraud, encompassing scams, phishing attacks, Ponzi schemes, and various other illicit activities. An increasing number of prominent legal cases and notable instances of cryptocurrency insolvencies highlight the importance of understanding the legal complexities associated with the broader cryptocurrency industry. While these issues often arise within centralized platforms and exchanges, they underscore the critical need to apply lessons learned from traditional banking and securities regulation to both centralized and decentralized components of the cryptocurrency landscape.²⁶¹ Transactions involving cryptocurrencies are purportedly characterized by greater privacy and are subject to less regulatory oversight compared to transactions conducted using conventional currencies. This has led to an attraction for fraudsters who exploit cryptocurrencies as a means to perpetrate their criminal activities²⁶². The DeFi sector, a rapidly expanding domain within the cryptocurrency space, anticipates achieving a Total Value of Cryptocurrency Locked (TVL) reaching an apex of \$250 billion in the year 2022. This noteworthy growth, however, has become a magnet for fraudulent activities perpetrated by nefarious entities. As elucidated in a comprehensive report by Elliptic, a blockchain analytics firm, the deleterious impact of DeFi scams manifested in a staggering loss surpassing \$10 billion during the period spanning January to November of 2021.

²⁶¹ Quadriga Fintech Solutions Corp, Whiteside Capital Corporation & 0984750 BC Ltd (1 April 2019), Halifax 484742 (NS SC), Termination and Bankruptcy Assignment Order.; Cred Inc, et al, Wilmington 20-12836 (Bankr D Del 09 November 2020).; Celsius Network LLC, Hoboken 22-10964 (Bankr D NY 13 July 2022).; Terraform labs Pte Ltd (Terra Luna) (23 September 2022), Singapore HC/OC 247/2022 (SGHC [Gen Div]).; Voyager Digital Holdings, Inc, New York 22-10943 (Bankr D NY 05 July 2022).; Three Arrows Capital Ltd, New York 1:22-bk-10920 (Bankr D NY 01 July 2022).

²⁶² Udit Agarwal et al., "Blockchain and crypto forensics: Investigating crypto frauds" (2023) International Journal of Network Management, e2255, DOI: 10.1002.

Rest of the chapter endeavors to delve into prevalent instances of DeFi fraudulence, advocating for meticulous regulatory measures and robust oversight. Notably, malevolent actors within the realm of cryptocurrency often endeavor to gain unauthorized access to users' private information or coerce them into transferring assets to compromised digital wallets. The inherent challenge in combating such malfeasance lies in the intricate nature of blockchain technology, which, while featuring an immutable ledger that records all transactions, is also characterized by its privacy and decentralized structure. Although the ledger is transparent and unchangeable, the anonymity of participants and the use of techniques like mixing services or privacy coins can obscure the origins and destinations of stolen funds, making the traceability of those funds an arduous task.

DeFi scams can be categorized into two principal groups. The first pertains to scams involving users directly transferring assets to fraudulent crypto wallets, often arising from impersonation or fraudulent investment schemes such as "Rug Pulls." The second category involves malicious actors acquiring access to users' wallets or sensitive information, including private keys, sometimes through the theft of physical wallets, specifically cold wallets which are offline storage devices designed to keep cryptocurrency secure. Subsequently, these malevolent actors carry out the transfer of crypto assets to alternative wallets. The thesis will discuss these two phenomena, but primarily focus on fraudulent DeFi projects and investment issues, where malevolent actors entice unsuspecting crypto holders into spurious investment or business opportunities. These deceptive practices typically involve promises of extraordinary returns with rapid return on investment ("ROI"), leading investors to discover the impossibility of withdrawing their funds post-investment, especially when they have entered too late in a Ponzi scheme. In dissecting the multifaceted realm of cryptocurrency fraudulence within the DeFi landscape, this thesis will analyze various types of risks brought about by fraudulent activities, including hacking for cryptocurrency theft, high yield investment programs ("HYIPs"), Ponzi Schemes, Rug Pulls, The "Pump and Dump," The Honey Pot, Scams in Cloud Mining, and ICO scams. Understanding

the nuances and *modus operandi* of each of these fraudulent schemes is crucial as it equips investors and stakeholders with the knowledge needed to recognize and mitigate the associated risks, thereby safeguarding their investments and fostering a more secure DeFi ecosystem.

A. Hacking for Cryptocurrency Theft.

Hackers employ various tactics to pilfer cryptocurrencies from investment accounts, exploiting vulnerabilities despite the security measures inherent in blockchain technology, such as passwords, private keys, or access codes. They can siphon cryptocurrency from investors' crypto wallets by obtaining or compromising these private keys, fabricate fake wallets to deceive counterparties, or establish sham cryptocurrency exchanges to unlawfully obtain consumers' funds. Even with the use of passwords and other security protocols, these sophisticated attacks can lead to significant losses for unsuspecting investors.²⁶³ Cryptocurrency exchanges, in particular, remain susceptible to cyberattacks, with numerous breaches occurring regularly. Notably, Mt. Gox, a prominent exchange, fell victim to hacking twice—first in 2011 and then in 2014—demonstrating the potential for severe destabilization within the exchange ecosystem²⁶⁴. Instances like the \$320 million loss suffered by the BTC exchange company Wormhole in February 2022 underscore the significant impact of cyberattacks on the cryptocurrency market. Unfortunately, such incidents have become increasingly common since 2021, with the Federal Trade Commission's investigations revealing over \$1 billion in cryptocurrency fraud losses within a relatively short time frame. BTC emerges as a prevalent payment method in fraudulent activities, with the FTC's data indicating its involvement in 24% of all dollar losses reported in fraud incidents between January 1, 2021, and March 31, 2022²⁶⁵. In numerous instances, cyber attackers take advantage of vulnerabilities in newly constructed DeFi systems to pilfer funds from users of DeFi protocols²⁶⁶.

²⁶³ Ibid.

²⁶⁴ Bodkhe et al., "Blockchain for precision irrigation: opportunities and challenges" (2022) *Transactions on Emerging Telecommunications Technologies* 33(10), e4059

²⁶⁵ Udit Agarwal et al., (2023), see note 262

²⁶⁶ Ibid.

Furthermore, cyberattacks targeting cryptocurrencies amplify both the volatility of the compromised currency and the interconnections between different cryptocurrencies²⁶⁷. Substantial regulatory measures, surveillance mechanisms, and enforcement actions are imperative to safeguard all cryptocurrencies, considering the internal disruptions they generate and the potential spill-over effects onto other interconnected crypto markets. This aligns with the trend towards adopting a comprehensive global framework for financial regulation²⁶⁸. Thus, regulatory measures and surveillance are indeed crucial for managing these risks and aligning with broader financial regulation trends. While substantial regulatory measures are crucial for safeguarding cryptocurrencies, assessing the feasibility of a comprehensive global framework remains important. Implementing a global regulatory framework is challenging due to varying national laws, the decentralized nature of cryptocurrencies, and potential economic impacts. Despite these hurdles, international initiatives like those by the FATF aim to promote greater regulatory alignment, which is essential for effective oversight. The decentralized structure of cryptocurrency facilitates the direct transfer of value between parties without the involvement of intermediaries, allowing for remote and anonymous ransom payments²⁶⁹. Incidents of cryptocurrency hacks are associated with abnormal returns in the hours leading up to the actual hacking event; however, these abnormal returns tend to dissipate and return to zero upon the public disclosure of the hack²⁷⁰. This observation indicates that existing regulatory and surveillance measures may be insufficiently prompt to effectively protect investors.

B. High Yield Investment Programs (“HYIPs”)

HYIPs are unauthorized investment opportunities often operated by unlicensed individuals. These schemes promise high returns with minimal or no risk to investors, a hallmark

²⁶⁷ Corbet, Shaen, Douglas John Cumming, Brian Lucey, Maurice Peat, and Samuel Vigne, "Investigating the Dynamics between Price Volatility, Price Discovery, and Criminality in Cryptocurrency Markets" (Working Paper, Rochester: SSRN, 2018).

²⁶⁸ Ka Kei Chan and Alistair Milne, "The Global Legal Entity Identifier System: How Can It Deliver?" *Journal of Risk and Financial Management* 12 (2019): 39.

²⁶⁹ Douglas J. Cumming, Sofia Johan, and Anshum Pant (2019), see note 284.

²⁷⁰ Corbet, Shaen et al., (2018), see note 279.

characteristic of HYIP scams. Typically, an HYIP website will advertise extravagant returns, such as 30% or 40% annually (or even more) on investments. Some may even claim association with a "prime bank" initiative to add an air of legitimacy. HYIPs frequently leverage cryptocurrency assets and rely on a pyramid-like structure, where existing investors are incentivized to recruit new participants²⁷¹. From a legal perspective, HYIPs raise significant concerns regarding investor protection and financial regulation. Firstly, the lack of authorization and licensing implies a breach of regulatory requirements, rendering these schemes illegal in many jurisdictions. Moreover, the promise of high returns with little to no risk is often deceptive, potentially constituting fraudulent misrepresentation or false advertising under consumer protection laws.

The research conducted by J. Neisius and R. Clayton sheds light on the fraudulent practices within HYIPs, particularly their use of selective payments to deceive investors²⁷². By paying returns only to aggregators or selected investors while withholding payments from others, these schemes perpetrate fraud and undermine trust in financial markets. Similarly, Toyoda et al.'s exploration of clustering algorithms to detect relationships between HYIP websites underscores the deceptive nature of these schemes²⁷³. Their findings reveal how interconnected these fraudulent operations can be, often controlled by the same individuals or entities. This interconnectedness serves to deceive investors by creating an illusion of legitimacy or diversification when, in reality, the schemes are part of a coordinated effort to defraud unsuspecting individuals. HYIPs represent a significant legal challenge, as they often involve outright criminal activities, including fraud and deception, that exploit unsuspecting investors. Since these schemes inherently operate outside regulatory frameworks, addressing them requires not only robust enforcement of financial regulations but also enhanced transparency measures and

²⁷¹ Udit Agarwal et al., (2023), see note 262

²⁷² J. Neisius & R. Clayton, "Orchestrated crime: the high yield investment fraud ecosystem," in 2014 APWG Symposium on Electronic Crime Research (ECRIME) (IEEE, 2014), pp. 48-58.

²⁷³ Kentaroh Toyoda et al., "A novel methodology for HYIP operators' bitcoin addresses identification," *IEEE Access* (2019), 7: 74835-74848.

public awareness campaigns. Educating investors about the risks associated with such schemes is crucial in preventing them from falling victim to these illegal operations.

C. Ponzi Schemes

Ponzi schemes are fraudulent investment operations where purported profits for existing investors are paid out using funds acquired from new investors. These schemes promise substantial returns with little or no risk, enticing fresh investors to participate. However, rather than engaging in legitimate investment activities, operators of Ponzi schemes focus on gathering new funds to meet payouts promised to earlier investors while diverting portions of these funds for personal gain. Examples include:

- BitConnect, founded in 2016, operated as a BTC lending service offering monthly returns of up to 40%. Investors could lend their cryptocurrencies to the platform in exchange for significant profits based on the duration of the loan. With its multi-level marketing structure and extravagant rewards (including 1% daily compounded interest), BitConnect faced accusations of operating as a Ponzi scam. The scheme collapsed in 2018, resulting in losses of \$3.5 billion for investors²⁷⁴.
- OneCoin, presented as a cryptocurrency by OneCoin Ltd and OneLife Network Ltd, operated as a Ponzi scam disguised as an MLM initiative²⁷⁵. Although the company provided educational resources on cryptocurrency, these materials were part of a broader marketing strategy. Participants were incentivized to recruit more individuals, with rewards awaiting successful recruiters. The company purportedly generated \$4 billion in revenue from 2014 to 2016²⁷⁶.

²⁷⁴ United States, Department of Justice, Southern District of California, *Founder of Fraudulent Cryptocurrency Charged in \$2 Billion BitConnect Ponzi Scheme* (25 February 2022), online: <https://www.justice.gov/usao-sdca/pr/founder-fraudulent-cryptocurrency-charged-2-billion-bitconnect-ponzi-scheme>.

²⁷⁵ United States, Department of Justice, Southern District of New York, *Co-Founder of Multi-Billion-Dollar Cryptocurrency Pyramid Scheme "OneCoin" Pleads Guilty* (16 December 2022), online: <https://www.justice.gov/usao-sdny/pr/co-founder-multi-billion-dollar-cryptocurrency-pyramid-scheme-onecoin-pleads-guilty>.

²⁷⁶ Ibid

- PlusToken, heavily promoted through the Chinese messaging app WeChat, enticed investors with promises of monthly returns ranging from 10% to 30%. Despite drawing nearly three million investors, primarily from China, South Korea, and Japan, PlusToken operated as a fraudulent scheme, resulting in losses exceeding \$3 billion before being shut down in 2019²⁷⁷.

Canadian securities laws prohibit fraudulent schemes, including Ponzi schemes, by requiring securities issuers and dealers to be registered and by imposing disclosure and reporting obligations. Moreover, the CSA provides investor education and alerts to raise awareness about potential investment scams²⁷⁸. To mitigate the risks associated with these schemes, Canadian regulators regularly issue warnings to investors about suspicious investment opportunities and fraudulent schemes. Additionally, enforcement actions can be taken against individuals and entities found to be operating illegal investment schemes.

D. Rug Pulls

A quintessential example of prevalent DeFi scams is the "Rug Pull." These elaborate schemes involve developers promoting seemingly revolutionary crypto projects to garner substantial investments. Upon accumulating considerable funds, these developers abscond with the capital, often facilitated by programming back doors into the project's smart contracts or exploiting liquidity pools, thereby rendering investors with valueless tokens. Rug pulls are a prevalent tactic employed within DEXs, which are the DeFi counterparts of traditional market exchanges. Notably observed in platforms like Uniswap, rug pulls involve fraudulent actors creating an Ethereum Request for Comments 20 ("ERC-20") token and listing it on a DEX, often pairing it with a dominant cryptocurrency such as USD or Ether. Uniswap operates on the Ethereum blockchain as an on-chain liquidity protocol, facilitating trustless token swaps where all

²⁷⁷ Shaen Corbet, ed, *Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies* (Berlin: De Gruyter, 2022), online: <https://doi.org/10.1515/9783110718485>.

²⁷⁸ Ontario Securities Commission (OSC), "Canadian securities regulators issue warning about fraudulent investment solicitations involving crypto assets," News release, January 17, 2022, <https://www.osc.ca/en/news-events/news/canadian-securities-regulators-issue-warning-about-fraudulent-investment-solicitations-involving>.

transactions occur via smart contracts without the need for intermediaries or trusted parties²⁷⁹. After attracting investors and inflating the token's value, the scammers withdraw all the liquidity from the pool, leaving investors with worthless tokens and absconding with the funds. Identification of "Rug Pulls" necessitates vigilance for key indicators, including low to no team credibility, ambiguous white papers, unrealistic projections, excessive marketing, and promotion strategies, as well as a scarcity of token holders or listing on a singular DEX. Furthermore, in 2021, there was a notable trend in NFTs, marked by an extraordinary 1,785% rise in market capitalization. Yet, this heightened popularity rendered NFTs susceptible to rug pull scams, leading to several NFT projects falling prey to such fraudulent schemes.

E. The "Pump and Dump"

Another pervasive DeFi scam is the "Pump and Dump," wherein worthless assets are artificially inflated through orchestrated marketing, subsequently resulting in significant losses for unwitting investors²⁸⁰. The "Pump and Dump" stratagem capitalizes on inducing swift investments by leveraging immediate hype. Potential investors are advised to scrutinize the purpose of the coin, as pump and dump coins often lack a substantive use case. Caution is recommended against succumbing to social media hype and unfounded rumors, underscoring the imperative to conduct thorough research.

F. The "Honey Pot"

The Honey Pot scam, akin to the *modus operandi* of pump and dump scams, distinguishes itself by confining the ability to sell holdings exclusively to the developers. The architects of these scams entice investors with exaggerated price projections and strategic marketing, fostering a surge in asset prices as more individuals invest, ostensibly propelling the value "to the moon." The predicament ensues when investors endeavor to realize their profits, encountering error messages

²⁷⁹ Udit Agarwal et al., (2023), see note 262

²⁸⁰ The U.S. Commodity Futures Trading Commission (CFTC), "Customer Advisory: Beware Virtual Currency Pump-and-Dump Schemes," https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_pumpdump0218.pdf

such as "transactions can't succeed due to error undefined; this is probably due to a problem with one of the tokens you're swapping." This predicament arises from a malevolent insertion of code within the smart contract, rendering it unfeasible for investors to divest themselves of their holdings. Discerning a Honey Pot scam mandates the same level of vigilance as with Rug Pulls and Pump and Dump schemes, necessitating thorough due diligence before committing to any DeFi project. In this context, potential investors are advised to scrutinize project details, conduct comprehensive research, and remain attuned to warning signs indicative of deceptive practices.

- ***Scams in Cloud Mining***

Within this investment scheme, fraudulent platforms persuade investors and individual buyers to contribute initial capital with the promise of securing a continuous allocation of mining power. Cloud mining enterprises offer the option to lease mining hardware, which they undertake to manage for a predetermined initial payment. In exchange, investors receive a portion of the generated revenue, enabling them to engage in remote mining without the need to acquire costly hardware. The crux of the issue lies in the deceptive nature of cloud mining scam entities. Contrary to their claims, these platforms do not possess the purported hash rate. Consequently, investors stand to incur losses as their capital is unrecoverable, and the anticipated returns on their initial payment remain unrealized.

G. Initial Coin Offering Frauds

ICOs, as unregulated fundraising mechanisms for crypto projects, are susceptible to fraudulent activities. However, a key distinction between IPOs and ICOs is that while an IPO is typically conducted by a company that has undergone significant regulatory scrutiny and has an established business model, an ICO is often launched by new ventures that may carry higher risks due to their early-stage development and lack of regulatory oversight. In the case of fraudulent ICOs, numerous scams have emerged where businesses disappeared after receiving significant amounts of funds²⁸¹. In ICO scams, investors are deceived into purchasing tokens at ostensibly

²⁸¹ Udit Agarwal et al., (2023), see note 262

discounted prices, only to be deprived of their token shares when the project proves to be illegitimate. Developers behind such scams may employ deceptive tactics, including high-level marketing and counterfeit legal documentation, to create a façade of legitimacy.

- **Innovation Versus Fraud**

Satoshi Nakamoto explains that the blockchain achieves consensus by virtue of the longest chain. For a malicious attack to succeed, a fraudulent node would need to redo the work of the targeted block and all subsequent blocks, surpassing the collective work of honest nodes. Nakamoto demonstrates that as subsequent blocks are added, the likelihood of a slower attacker catching up decreases exponentially²⁸². In the conventional realm of fundraising, companies pioneering innovative products or services typically must create a prototype or beta version to prove the concept's viability to potential investors. After demonstrating the product's functionality, and often after some degree of adaptation, a company can pursue venture funding to further develop or scale the concept. However, this often necessitates entrepreneurs relinquishing a significant portion of equity in their ventures in exchange for initial seed capital. This dynamic creates barriers for entrepreneurs lacking access to a network of affluent accredited investors and restricts investment opportunities primarily to this privileged group. Under Canadian securities law, the "accredited investor exemption" allows certain individuals and entities who meet specific income, asset, or professional criteria to invest in securities without the issuer needing to file a prospectus or adhere to some of the standard regulatory requirements²⁸³. This exemption, while facilitating access to capital for established investors, often excludes a broader range of potential investors from participating in these opportunities.

ICOs represent a significant departure from this traditional model by revolutionizing how ideas are conceived and brought to market. They enable developers with promising ideas for blockchain-based applications, products, or services to raise capital directly from the individuals

²⁸² Nakamoto (2008), see note 28.

²⁸³ See National Instrument 45-106 *Prospectus Exemptions*, s 2.3, which outlines the criteria for "accredited investors" under Canadian securities law.

or entities who stand to benefit from the eventual product or service²⁸⁴. The tokens issued in an ICO do not confer any ownership rights or equity in the company conducting the offering. Instead, ICOs typically issue tokens that serve a specific purpose within the software program or ecosystem being developed. These tokens often have utility within decentralized applications on the blockchain or can be used to acquire goods or services within the issuing entity's decentralized software or protocol. While primarily intended for use within the issuing entity's blockchain ecosystem, these application tokens may also function as a standalone store of value, tradable on various online cryptocurrency exchanges. Consequently, ICOs differ significantly from IPOs and are more akin to pre-orders, wherein investors acquire assets that will have value within the issuing entity's system once it is developed, if indeed it materializes²⁸⁵.

The clash between innovation and fraud is an intricate dynamic that underscores the perpetual challenge in technologically progressive landscapes. As innovation paves the way for novel and transformative solutions, it concurrently offers fertile ground for opportunistic individuals to engage in fraudulent activities. The fast-paced evolution of technologies, particularly in sectors like fintech and DeFi, introduces vulnerabilities that cunning actors exploit. Striking a delicate balance between fostering innovation and erecting robust safeguards against fraud becomes imperative. Regulatory frameworks and cybersecurity measures must evolve in tandem with technological advancements to nurture innovation while fortifying defenses against fraudulent schemes, thus fostering a secure environment for progress.

- **Fighting DeFi Fraud: Legal Safeguards for Investors.**

International regulators, notably International Organization of Securities Commissions (“IOSCO”), are exploring concerns related to market manipulation, fraud, and abusive practices targeting consumers²⁸⁶. These conventional regulatory concerns extend to the stablecoin realm and

²⁸⁴ Douglas J. Cumming, Sofia Johan, and Anshum Pant, "Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty," *Journal of Risk and Financial Management* 12, no. 3 (2019): 126, doi: 10.3390/jrfm12030126

²⁸⁵ Ibid

²⁸⁶ The Board of the International Organization of Securities Commissions, "Global Stablecoin Initiatives," Public Report, OR01/2020, March 2020, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf>.

the broader crypto-asset domain. However, stablecoin arrangements introduce additional apprehensions regarding investor protection due to their connection with fiat currency or other assets. Specifically, stablecoin issuers may be incentivized to invest in risky assets or loan out assets backing the stablecoin to achieve higher returns²⁸⁷. Without regulation, stablecoin issuers may profit by investing in higher-return or illiquid assets or by lending funds or assets while providing minimal or no interest to stablecoin holders. In the U.S., offering interest on stablecoins could classify them as securities, which would subject them to additional regulatory scrutiny. As a result, most stablecoin issuers avoid providing interest to holders to maintain their regulatory status. These incentives underscore the importance of asset segregation, collateral considerations, as well as market surveillance and disclosure frameworks.²⁸⁸

Combatting DeFi fraud requires a multi-faceted legal approach, as the decentralized and global nature of these schemes poses unique challenges. The following are some legal strategies that individuals or authorities might consider:

- **Regulatory Compliance:** Advocate for or work within existing regulatory frameworks. Encourage or participate in the development of regulations specific to the DeFi space, ensuring that platforms are accountable and comply with legal standards.
- **Global Coordination:** Collaborate with international regulatory bodies to establish a cohesive approach to address cross-border DeFi fraud. Given the borderless nature of cryptocurrencies, global coordination is crucial.
- **Educational Initiatives:** Promote awareness and education about the risks associated with DeFi investments. This can help potential investors make informed decisions and avoid falling victim to fraudulent schemes.

²⁸⁷ Jon Frost, Hyun Song Shin, & Peter Wierts, "An early stablecoin? The Bank of Amsterdam and the governance of money," BIS Working Papers, No. 902, November 10, 2020, <https://www.bis.org/publ/work902.pdf>

²⁸⁸ Douglas Arner, Raphael Auer, & Jon Frost, "Stablecoins: risks, potential and regulation," BIS Working Papers, No. 905, Monetary and Economic Department, November 2020, <https://www.bis.org/publ/work905.pdf>.

- **Blockchain Analytics and Forensics:** Engage blockchain analytics firms to trace transactions and identify patterns indicative of fraudulent activities. This can aid in investigations and provide evidence for legal actions.
- **Whistleblower Protection:** Establish or support mechanisms for whistleblowers to come forward with information about fraudulent DeFi schemes. Offering protection to individuals who expose wrongdoing can encourage reporting.
- **Collaboration with Exchanges:** Work with cryptocurrency exchanges to enhance due diligence processes and list only legitimate projects. Encourage exchanges to delist or flag suspicious tokens or projects.
- **Legal Actions:** Explore legal avenues for restitution and accountability. This may involve pursuing legal action against fraudulent developers or seeking compensation for victims through civil litigation.
- **Cooperation with Law Enforcement:** Collaborate with law enforcement agencies to investigate and prosecute DeFi fraud cases. Provide relevant information and support for criminal investigations.
- **Smart Contract Audits:** Encourage or mandate regular audits of smart contracts by reputable third-party security firms. This can help identify vulnerabilities and reduce the likelihood of exploitable weaknesses.
- **Industry Self-Regulation:** Promote self-regulatory measures within the cryptocurrency and DeFi industry. Establish industry standards and best practices that platforms voluntarily adhere to, fostering a more trustworthy environment.
- **Balancing of Innovation and Regulation**

In the realm of digital finance, just as regulators struggled to control the dissemination of information and knowledge, governments are now facing the challenge of containing the rapid advancement of blockchain-based technologies.²⁸⁹ For instance, Bitcoin, the first decentralized

²⁸⁹ Aaron Wright & Primavera De Filippi (2015), see note 27, p.29

cryptocurrency, has revolutionized the concept of digital currency by enabling peer-to-peer transactions without the need for intermediaries like banks. Its decentralized nature, facilitated by blockchain technology, poses unique regulatory challenges as traditional financial regulations struggle to adapt to this new paradigm. Likewise, the fluctuation of digital assets within a single day is notably affected by the timings of international trading, implying that comprehensive monitoring across various markets would aid in identifying potential market manipulation within cryptocurrency markets. Additionally, the fluctuation within a single day is impacted by periods of notable volatility in oil and exchange rate markets, underscoring the importance of extensive surveillance across different financial products to detect potential market manipulation within cryptocurrency markets²⁹⁰.

Furthermore, introduction of smart contracts has opened up new possibilities for DApps and DAOs, which operate without centralized control.²⁹¹ However, these advancements have also raised concerns among regulators about potential risks such as fraud, money laundering, and market manipulation. While security laws are vital for investor protection and market integrity, they may need to be reformed to accommodate the innovative potential of blockchain-based technologies. For example, the traditional securities registration process, aimed at ensuring transparency in fundraising, may be impractical for decentralized crowdfunding platforms like ICOs. ICOs allow projects to raise funds by issuing tokens on blockchain, bypassing financial intermediaries. However, when tokens qualify as securities, the global, decentralized nature of ICOs makes the registration process difficult, requiring detailed disclosures and compliance with various jurisdictional regulations, which are hard to align with the fast-paced and borderless nature of ICOs. The lack of clear regulatory guidelines further complicates matters, leading to uncertainty and inconsistency in how ICOs are treated across different jurisdictions. The reason for denying digital assets as securities stems from the lack of a third-party anticipating returns on investment,

²⁹⁰ Douglas J. Cumming, Sofia Johan, and Anshum Pant (2019), see note 284.

²⁹¹ Buterin, Vitalik. "A Next Generation Smart Contract & Decentralized Application Platform." Ethereum White Paper. 2013.

which in turn invalidates their classification as securities²⁹². The industry lacks significant historical comprehension, leading to a shortage of legal professionals dedicated to addressing its regulatory concerns. Additionally, the limited recognition of the technology's disruptive potential contributes to this gap. Lawyers often attempt to fit emerging technologies into pre-existing legal frameworks²⁹³. Regulation plays a pivotal role in fostering innovation²⁹⁴. However, as noted by Butenko and LaRouche (2015),²⁹⁵ regulatory frameworks and their effective enforcement often lag behind the pace of innovation. Scholarship in the realm of law and technology underscores the potential for innovation to yield harmful outcomes, while literature in law and economics primarily focuses on identifying market failures, enhancing information flow, and incentivizing innovation.²⁹⁶ Given the rapidly evolving nature of the cryptocurrency market and other entrepreneurial ventures utilizing blockchain technology, there arises a necessity for an integrated approach bridging the domains of law and technology with those of law and economics.

Blockchain applications operate within existing regulatory frameworks, meaning they cannot be entirely separated from legal and economic considerations. This interdependence highlights the need for careful evaluation from both law and economics perspectives. However, it's important to recognize that not all blockchain applications yield positive outcomes; some may facilitate illicit activities, such as money laundering or market manipulation. Addressing these potential risks requires a multidisciplinary approach that includes insights from law, technology, and economics, as well as effective regulatory oversight to balance innovation with security and compliance.²⁹⁷ In the nascent phase of legal and institutional advancements, extensive research is necessary to comprehensively grasp the suitable legal frameworks and surveillance/enforcement mechanisms that can mitigate adverse consequences stemming from blockchain applications

²⁹² Douglas J. Cumming, Sofia Johan, and Anshum Pant (2019), see note 284.

²⁹³ Ibid

²⁹⁴ Daniel F. Spulber, "Unlocking Technology: Antitrust and Innovation," *Journal of Competition Law* 4 (2008): 915–66

²⁹⁵ Anna Butenko and Pierre Larouche, "Regulation for Innovativeness or Regulation of Innovation?" *Law, Innovation and Technology* 7, no. 1 (2015): 52-82, doi: 10.1080/17579961.2015.1052643

²⁹⁶ Nicholas Crafts, "Regulation and Productivity Performance," *Oxford Review of Economic Policy* 22, no. 2 (Summer 2006): 186–202, doi: 10.1093/oxrep/grj012

²⁹⁷ Douglas J. Cumming, Sofia Johan, and Anshum Pant (2019), see note 284.

without impeding innovation. Moreover, there is a pressing need for further exploration into international cooperation and the harmonization of regulations, considering that blockchain-driven financial innovations often transcend national boundaries, operating with minimal regard for jurisdictional constraints²⁹⁸.

As cryptocurrencies such as bitcoin operate autonomously, free from geographical constraints and central bank influence, blockchain technology holds the potential to grant entrepreneurs worldwide access to startup capital and developmental funds. Building upon the foundations laid by disruptive funding methods like microfinance,²⁹⁹ blockchain has the capacity to advance these capabilities even further. By enabling a decentralized approach to financing, blockchain emerges as a pivotal enabler of entrepreneurship, a vital component of economic growth³⁰⁰. However, to realize its full potential, blockchain necessitates a regulatory framework that safeguards both investors and businesses³⁰¹, all the while fostering innovation and maintaining the facilitation of entrepreneurial financing.

To support the growth of innovative blockchain-based businesses, regulators may need to adopt a more flexible and adaptive approach to securities regulation. For instance, they could consider implementing regulatory sandboxes, where startups can test new products and services in a controlled environment with relaxed regulatory requirements. This approach allows regulators to closely monitor and evaluate emerging technologies while providing startups with the flexibility to experiment and innovate. While security laws play a crucial role in safeguarding investors and maintaining market stability, they should not stifle the potential of blockchain-based technologies to drive economic growth and innovation. By striking the right balance between regulation and

²⁹⁸ Ibid.

²⁹⁹ S. Bonini, V. Capizzi & P. Zocchi, "The Performance of Angel-Backed Companies" (2019) 100 *Journal of Banking & Finance* 328 at 328-345.

³⁰⁰ Aki Tomizawa et al, "Economic Growth, Innovation, Institutions, and the Great Enrichment" (2020) 37:5 *Asia Pacific Journal of Management*, online: <https://doi.org/10.1007/s10490-019-09648-2>.

³⁰¹ Mike W Peng et al, "An Institution-Based View of Global IPR History" (2017) 48:7 *Journal of International Business Studies* 893 at 893-907, online: https://ideas.repec.org/a/pal/jintbs/v48y2017i7d10.1057_s41267-016-0061-9.html.

innovation, policymakers can create a conducive environment for the development of a vibrant and sustainable blockchain ecosystem.

Chapter VIII: Consumer protection considerations: disclosure, transparency, privacy and cybersecurity.

DeFi has gained significant traction, attracting interest from both ordinary investors and users of financial services who seek novel avenues for engaging with assets, from artwork to enhanced trade execution and higher interest rates. However, being a fledgling industry with technology still in its developmental phase it is not without its risks³⁰². Similar to other financial sectors, issues such as counterparty risk, cybersecurity vulnerabilities, liquidity concerns, inadequate intellectual property protection, and more, pose threats to customer value and investor returns³⁰³.

Conventional financial oversight has developed over decades of monitoring entities acting as central intermediaries in financial transactions among customers, clients, and investors³⁰⁴. DeFi, however, operates on the basis of rule-bound, encoded protocols enforced redundantly by numerous independent entities³⁰⁵. Unlike centralized systems where transaction participants rely on mutual trust or third-party intermediaries for successful transactions, DeFi employs computer programs that eliminate discretion from technical operations. As was mentioned earlier, in DeFi transactions, automated agreements known as smart contracts are crafted using computer programming languages. These contracts are enacted on a digital ledger called a blockchain, which is replicated and dispersed across a network of computers. Smart contracts are designed with transactional rules encoded within them, enabling them to automatically execute specific functions when predetermined conditions are met. While they function as contracts in the sense that they enforce agreed-upon terms between parties, they may not always be legally binding in the traditional sense, depending on the jurisdiction and specific legal frameworks. These functions are carried out without human intervention upon the occurrence of relevant events or developments,

³⁰² Chris Brummer, (2022) See note 5

³⁰³ Ibid

³⁰⁴ Ibid

³⁰⁵ Wharton Blockchain and Digital Asset Project, "DeFi Beyond the Hype: The Emerging World of Decentralized Finance" (May 2021), available at <https://wifpr.wharton.upenn.edu/wpcontent/uploads/2021/05/DeFi-Beyond-the-Hype.pdf>.

but their legal enforceability can vary.³⁰⁶ As smart contracts are deployed on blockchains rather than centralized servers, their code, execution history, and operations are distributed, openly visible, and irreversible³⁰⁷.

Essentially, a cryptocurrency wallet, also known as a crypto wallet, serves as a means for individuals to engage with a blockchain network. Contrary to common belief, these wallets do not physically hold cryptocurrencies. Instead, they function as a conduit to the Blockchain network, providing the necessary tools for interaction. They enable the generation and processing of information required for cryptocurrency transactions. Typically, these systems generate multiple pairs of private and public keys, along with various Blockchain addresses. It's customary to employ seed phrases preceding these keys for added security. During transactions, cryptocurrencies remain within the Blockchain and are merely transferred between addresses following the verification of exchanged keys and validation by the network³⁰⁸.

In practice, exchange wallets are widely utilized. These wallets entail users creating accounts on digital platforms operated by service providers, often referred to as Exchanges. These accounts typically employ various security measures such as passwords, passcodes, and two-factor authentication, with optional biometric authentication. However, the management of currency and the necessary keys rests with the service provider; the Exchange generates a wallet address for the user, which can be controlled through the provided interface. While this setup offers convenience, there are considerations to bear in mind. Notably, the security of the user's funds relies not only on the integrity of their profile authentication but also on the security and trustworthiness of the platform itself.³⁰⁹ Should passwords or similar credentials be compromised, all funds become vulnerable. Even with two-factor authentication in place, individuals with knowledge or access to the user's information could exploit the system. Moreover, Exchanges retain the authority to freeze

³⁰⁶ Chris Bummer (2022), see note 5

³⁰⁷ Lily Francus (2022), see note 126

³⁰⁸ Mohamed Azman and Kunal Sharma, "HCH DEX: A Secure Cryptocurrency e-Wallet & Exchange System with Two-way Authentication," in 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (Tirunelveli, India: IEEE, 2020), 305-310, doi: 10.1109/ICSSIT48917.2020.9214122.

³⁰⁹ Ibid

or withhold user funds, contradicting the decentralized ethos³¹⁰. Consequently, there is a growing interest in DEXs, which operate without central authority and facilitate peer-to-peer transactions³¹¹.

Despite DeFi's goal of eliminating centralized intermediaries, the specialized knowledge required for managing private keys and interacting with the blockchain poses challenges for retail users aiming to directly engage with the DeFi system. Consequently, centralized, non-transparent, and unregulated intermediaries, referred to as CeFi, have emerged. These CeFi platforms operate differently from their DeFi counterparts by relying on human management rather than smart contracts. This reliance exposes investors to custodian risk and a lack of transparency. There are arguments that highlight that certain DeFi initiatives designate a particular entity with administrative privileges, enabling them to adjust the protocol at their discretion through private keys known as "admin keys".³¹² The presence of such "admin keys" raises concerns about the extent of decentralization. The possessor of the "admin key" holds the authority to modify programs and parameters associated with the DeFi project without requiring external approval³¹³. In certain instances, the term "decentralized" may merely serve as a marketing tool, with the reality being that many DeFi systems are either centralized or exhibit near-centralization. Nevertheless, if there isn't a central operator in place, there exists no entity to adhere to enforcement measures³¹⁴.

- **Balancing Decentralization with Accountability in DeFi Systems.**

A DeFi system may lack a central authority or have minimal control over its operations. In these instances, regulatory measures aimed at halting the illegal activity directly may be more effective than penalizing the entity to ensure compliance. Given that "decentralized" does not mean there is no accountability in cases of illegal activities, DeFi applications should incorporate

³¹⁰ Ibid.

³¹¹ Ibid.

³¹² R. Ushida & J. Angel, "Regulatory considerations on centralized aspects of DeFi managed by DAOs", in M. Bernhard et al. (eds.), FC 2021, LNCS, vol. 12676, Springer, Heidelberg (2021), pp. 21–36, https://doi.org/10.1007/978-3-662-63958-0_2. ; BGIN (Blockchain Governance Initiative Network), "Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations", BGIN SR 001 (2021).

³¹³ Tomonori Yuyama, Ken Katayama & Paul Brigner (2023), see note 75.

³¹⁴ Ibid.

mechanisms for correcting or ceasing such activities on their own³¹⁵. DeFi entities involved in the disclosure platform should undergo an annual audit. The audit summary should be made public on the disclosure platform, clearly verifying the entity's compliance as a proper DeFi. Establishing a standardized auditing protocol, approved by the disclosure platform, is recommended³¹⁶.

- **Highlighting a disparity: Professional vs. Retail Investors.**

In numerous DeFi initiatives, financial backing primarily stems from venture capital entities and seasoned investors³¹⁷. However, there exists ambiguity regarding the extent of comprehension among smaller investors regarding this dynamic. As highlighted by Crenshaw,³¹⁸ professional investors bring along a plethora of entitlements including equity stakes, options, direct engagement with project management, participation in governance structures (be it formal or informal), safeguards against dilution, and control prerogatives, often undisclosed to the broader public. Conversely, their involvement significantly influences the value of investments. Thus, it becomes apparent that venture capital does not necessarily align with public interests such as safeguarding investors and consumers. Consequently, Crenshaw underscores the considerable disadvantage small investors face in comparison to their professional counterparts, accentuating the widening information asymmetry and its detrimental implications³¹⁹.

Even when DeFi functions within the realm of "financial services," the issue arises of whether its users enjoy the same safeguards as conventional investors in traditional financial systems. Essentially, the concern revolves around whether participants in DeFi markets are afforded equivalent protections as those engaging in traditional financial markets. Even within traditional finance, qualified and institutional investors are considered professionals and thus accountable for their investment decisions. However, to facilitate informed judgments by professional investors, comprehensive explanatory materials and disclosures are imperative.

³¹⁵ Ibid.

³¹⁶ Ibid.

³¹⁷ Ibid.

³¹⁸ Crenshaw, C.A. (SEC Commissioner), "Statement on DeFi Risks, Regulations, and Opportunities," The United States Securities and Exchange Commission (2021).

³¹⁹ Ibid.

Consequently, implementing a framework that enables such investors to make sound investment choices becomes essential³²⁰.

- **Risk Disclosure.**

Implementing a robust disclosure mechanism will mitigate the opacity prevalent within DeFi, facilitating informed decision-making for investors. Disclosure is deemed essential not only for investors but also for consumers, even in the case of commonplace products. Therefore, it is imperative for DeFi to enhance its disclosure practices significantly³²¹. The existence of risks naturally raises the question of whether DeFi project founders are obligated to disclose such risks to end users. The answers to this question are not straightforward. Discussions regarding disclosure and DApps often revolve around whether smart contracts or protocols interact with securities, potentially triggering obligations to register as broker-dealers, exchanges, or investment companies³²². Similarly, there's a debate about whether a transaction constitutes the issuance of securities, which hinges on whether the transaction's economic realities collectively form an investment contract under securities laws. In cases where infrastructure serves as intermediaries for securities or facilitates their trading, securities laws impose substantive operational requirements concerning liquidity, leverage, and other factors. Conversely, transactions involving the issuance of securities trigger extensive disclosure requirements. These requirements encompass details about the issuer's operations, the use of proceeds from fundraising, management's narrative discussion, and more³²³. In the DeFi ecosystem, a key analytical concern frequently revolves around determining whether the entirety of the economic circumstances surrounding a transaction collectively constitute an "investment contract," a notion introduced in the seminal case of *Pacific Coast Coin Exchange v. Ontario Securities Commission*³²⁴.

³²⁰ Tomonori Yuyama, Ken Katayama & Paul Brigner (2023), see note 75.

³²¹ Ibid

³²² Chris Bummer (2022), see note 5

³²³ Ibid.

³²⁴ *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] See note 219

The regulatory framework concerning disclosure primarily centers on different versions of the information consumers or investors require to make well-informed choices. However, it's not always clear to what degree entities are obligated by law to engage in specific disclosure practices enforced by the government. DApps may be subject to different regulatory frameworks regarding disclosure, contingent upon their specific context³²⁵. Even in cases where decentralized applications fall clearly under the oversight of the nation's main disclosure regulator, such as the governmental bodies who oversee securities' industry, the obligations regarding disclosure can be unclear and often does not account for the unique aspects of blockchain infrastructures³²⁶. Scholars argue that securities law and consumer protection regulations vary not only in their operational aspects but also in their substance. Securities law relies on extensive submissions intended for analysis by institutional entities, whereas consumer protection regulation emphasizes concise, user-friendly disclosures tailored for everyday consumers to easily understand³²⁷. Modern securities law primarily revolves around extensive disclosure, primarily targeting institutional investors and courts for potential future liabilities, rather than retail investors. Retail investors are seen as receiving indirect benefits from disclosure, either through sellers of securities utilizing the information or by having the ability to pursue legal action against companies for deceptive disclosures that cause them harm.

In contrast, consumer protection-oriented disclosure strategies aim to directly benefit everyday consumers. These disclosures are designed to be comprehensible even to individuals lacking sophisticated financial knowledge, with the goal of preventing abuse and protecting against harm³²⁸. However, it is worth noting that, under both securities regulations and consumer protection laws, there is not an obligation to disclose every potential risk to investors, which might also be practically impossible³²⁹. Instead, project curators must pinpoint the risks that are most

³²⁵ Ibid

³²⁶ Ibid p.139

³²⁷ Ibid

³²⁸ Ibid.

³²⁹ Ibid. p. 154

probable or, if less probable, would have the most significant impact on the functioning of the DeFi project³³⁰. This is particularly crucial for apps targeting consumers, as the user base increasingly includes individuals with limited financial sophistication. In such cases, risks may be intricate and not readily apparent, emphasizing the importance of clearly identifying and communicating the most significant risks³³¹. Project curators should go beyond simply stating "buyer beware" and provide contextualization for the risks they identify. Additionally, they should clearly and concisely explain in straightforward language the measures they have implemented to mitigate these risks³³².

- **Clarity in DeFi Documentation**

In the realm of cryptocurrency, the traditional means of disclosure, namely white papers, have faced criticism for being both challenging to comprehend and frequently exaggerated. White papers, used to communicate information about cryptocurrency technology, often contain assertions that are difficult to distinguish as either hopeful projections or practical realities. While they may provide intricate technical details about a project, they often lack accompanying explanations or statements to clarify these details. Moreover, while white papers may occasionally include references to contractual terms and conditions, they predominantly emphasize the potential societal impact of the technology rather than its practicalities. This tendency is exacerbated in an era dominated by brief and exaggerated communication on platforms like Twitter and other social media. Consequently, even individuals with technical expertise may struggle to decipher such disclosures, leaving retail investors, particularly those with limited understanding, with insufficient actionable insights³³³.

For example, when promoting a Dapp as an investment opportunity, it's essential that the investment nature of the Dapp is transparently disclosed, accompanied by a clear explanation of how and why it constitutes an investment. Additionally, if a Dapp offers financial services, such

³³⁰ Ibid. p. 154

³³¹ Ibid. p. 161

³³² Ibid. p. 161

³³³ Ibid, p. 156

as "crypto pair trades," these services should be succinctly described in straightforward language to ensure users grasp their nature. The disclosures should align with the dapp's business model, outlining how and when users stand to benefit from utilizing the application³³⁴. If a Dapp is designed to facilitate profit generation in any form, it's crucial to provide detailed explanations of how earnings are generated. For instance, if users are expected to earn returns through activities like mining (i.e., validating new transactions on the blockchain), staking (committing crypto assets to support a blockchain network and validate transactions), providing liquidity, funding rates, or other innovative methods such as gaming proceeds, entrepreneurs should thoroughly explain each concept. Moreover, since these processes might involve third-party institutions or procedures, they should also be disclosed and clarified, including how earnings are anticipated to be realized³³⁵.

Given that most end users and investors typically require some form of token to engage with, possess, and invest in DeFi projects and services, including activities like purchasing NFTs, participating in gaming, or initiating smart contract operations and DApps, it becomes imperative to provide transparent disclosure regarding token economics and functionality, particularly in instances where tokens are acquired as investments. Initially, the fundamental economics of a token should be clearly outlined, covering aspects such as factors influencing token supply and demand. Entrepreneurs should consider, if available, the planned total token supply, token divisibility, and any token lockups, especially those held by founders or insiders, as their release could inflate the token supply. Additionally, founders should disclose whether they or another entity have the authority to issue more tokens, or alternatively, to redeem or eliminate tokens in the future. Likewise, users holding utility tokens should be informed if the expected utility, as marketed to them, is subject to alteration or compromise due to changes in the DApp or protocol code. Furthermore, any factors impacting the token's market, consumption, or investment value should be transparently disclosed³³⁶.

³³⁴ Ibid, page. 153

³³⁵ Ibid.

³³⁶ Ibid, p. 156

DApps are required to disclose the fundamental characteristics of any crypto tokens essential for their operational functionality. For stablecoins, consumers should be informed about the assets held in reserve to support the coins, as well as whether their funds will be lent out or pooled with others for investment purposes. In cases where cryptocurrencies are issued, sold, or lent as platform or rights tokens, consumers should be informed about the privileges granted to token holders, along with any restrictions or redemption rights affecting the token's liquidity. Additionally, promoters, where applicable, should offer comprehensive disclosures regarding their methods for securing and storing private keys³³⁷.

Any conflicts of interest inherent in the token economy must also be transparently disclosed³³⁸. Governance mechanisms for DApps and tokens can vary significantly, potentially resulting in misaligned incentives between platform investors, such as liquidity providers or lenders, and platform governors³³⁹. In certain cases, investors holding substantial governance token stakes may prioritize promoting long-term platform health, which may conflict with the interests of short-term investors or end users. For instance, governance tokens distributed to stakeholders might be destroyed or sold in treasury operations to maintain platform stability. While such actions may be in the best interest of the application overall, they should be fully disclosed to end users or investors in the token³⁴⁰.

In regulatory contexts, disclosure entails not just the availability of information to the public, but also its comprehensibility. Regulatory scrutiny extends beyond the mere technical aspects of disclosure to encompass both the substance and manner in which information is conveyed. Consequently, while blockchain transparency prompts policymakers to rethink the objectives of disclosure—especially considering that sophisticated parties largely have access to

³³⁷ Ibid, p. 157

³³⁸ Ibid.

³³⁹ Lily Francus (2022), see note 126

³⁴⁰ "Ethereum Explanatory Document (2024), see note 124.

available information—merely making information accessible for review does not guarantee effective disclosure³⁴¹.

³⁴¹ Chris Bummer (2022), see note 5, page. 161

Chapter IX: Tax Treatment of Virtual Assets

The Government of Canada's official website provides comprehensive tax information regarding crypto-assets, with specific emphasis on the most common tax issues related to these assets. The website distinguishes various types of crypto-assets, including cryptocurrencies, utility tokens, security tokens, and non-fungible tokens (NFTs), each serving different functions within their respective ecosystems. It further details the characteristics of crypto-assets and provides information on the amendments to the Excise Tax Act³⁴², specifically in section 188.2, defining "crypto assets" for the application of goods and services/harmonized sales tax (GST/HST) to cryptoasset mining activities³⁴³. Regarding tax considerations, the website advises that the tax treatment of a crypto-asset depends on various factors and must be determined on a case-by-case basis. It outlines the documentation required for crypto-asset mining activities and emphasizes the importance of keeping records. Additionally, the website discusses the determination of the value of a crypto-asset for tax reporting purposes. It provides guidance on reporting business income or capital gains resulting from crypto-asset transactions and offers examples to illustrate these concepts. The discussion covers considerations for determining inventory value and outlines the tax implications of earning crypto-assets through proof-of-work mining. The website concludes with information on applying GST/HST to cryptocurrency transactions, stating that the tax is calculated based on the fair market value of the cryptocurrency at the time of the exchange³⁴⁴.

Another guide from the Government of Canada website³⁴⁵ provides a concise overview regarding virtual currency and its tax implications. It addresses the various uses of virtual currency, such as buying goods, functioning as a commodity, paying employees, and earning through mining or staking. Specifically, it explains that virtual currency refers to a digital asset designed for buying

³⁴² Excise Tax Act, RSC 1985, c E-15, <https://laws-lois.justice.gc.ca/eng/acts/e-15/>.

³⁴³ Budget Implementation Act, 2023 (the BIA), S.C. 2023, s. 188.2 (Can.).

³⁴⁴ Government of Canada, "Cryptocurrency Guide," Canada Revenue Agency, <https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html>.

³⁴⁵ Government of Canada. "Digital Currency - Information for crypto-asset users and tax professionals." Canada Revenue Agency, <https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency.html>.

and selling goods or services, with cryptocurrencies being a specific type based on blockchain technology. Examples include Bitcoin, and while numerous other cryptocurrencies exist, they are not regulated by central banks or countries, allowing for relatively anonymous transactions. Various transactions involving cryptocurrencies, such as buying or selling for traditional currency, transferring between individuals, or direct use for payments, may have tax implications.

When using virtual currency to purchase goods or services, income tax regulations treat the purchase as a barter transaction and are governed by the barter rules outlined in the Income Tax Act³⁴⁶. Barter transactions involve the exchange of goods or services without using legal tender, and the Canadian-dollar value of items bought with cryptocurrency must be included in the seller's income for tax purposes. This designation permits the buying and selling of digital currencies on Exchanges³⁴⁷. Additionally, for GST/HST registrants accepting cryptocurrency as payment, the fair market value of the consideration received must be determined to calculate GST/HST. Consequently, transactions involving digital currency necessitate sellers to include the value of goods purchased in their income for tax purposes.

Virtual currency can also function as a commodity that subjects resulting gains or losses to potential taxation as income or capital. Tax consequences may arise when gifting, trading, using cryptocurrency for purchases, or converting it to government-issued currency. When digital currency is used as a salary or wage payment, the amount received in Canadian dollars is included in the employee's income under subsection 5(1) of the Income Tax Act³⁴⁸.

Mining, involving solving mathematical problems to confirm cryptocurrency transactions, results in payments to miners in the validated cryptocurrency. Staking, an alternative consensus mechanism, also leads to earnings with potential tax implications. Both processes involve

³⁴⁶ Income Tax Act, RSC 1985, c 1 (5th Supp), <https://laws-lois.justice.gc.ca/eng/acts/i-3.3/>.

³⁴⁷ Douglas J. Cumming, Sofia Johan, and Anshum Pant (2019), see note 284.

³⁴⁸ Income Tax Act, RSC 1985, c. 1 (5th Supp), s. 5(1).

receiving payments for creating new cryptocurrency on the network and fees from transactions in the validated block³⁴⁹.

Navigating the taxation of DeFi transactions is a multifaceted challenge. While traditional methods of hiding income, such as using cash or offshore accounts, are well-known, the decentralized and pseudonymous nature of DeFi transactions introduces a different type of complexity. The use of online cloud wallets exemplifies the challenges in determining the tax jurisdiction of cryptoassets, calling for a nuanced and adaptive approach to taxation regulations in the rapidly evolving landscape of digital assets. These transactions often occur across multiple jurisdictions and without intermediaries, making it difficult for tax authorities to track and enforce compliance using conventional methods. Addressing the tax implications of DeFi requires innovative approaches to ensure that these decentralized transactions are appropriately accounted for within existing tax frameworks.

Moreover, the accounting treatment of Bitcoin, a prominent digital asset in the crypto space, adds another layer of complexity to the taxation landscape. Scholars³⁵⁰ have delved into the accounting issues related to Bitcoins, emphasizing the need for a clear understanding of how to account for Bitcoin in formal financial statements. The primary issues include determining whether Bitcoin should be classified as a currency, commodity, or intangible asset, how to measure its value given its volatility, and how to account for gains or losses in value over time. The dynamic nature of digital assets like Bitcoin requires continuous evaluation and adaptation of accounting practices to align with the evolving financial landscape. The use of online cloud wallets exemplifies the challenges in determining the tax jurisdiction of cryptoassets, calling for a nuanced and adaptive approach to taxation regulations in the rapidly evolving landscape of digital assets.

³⁴⁹ Government of Canada. "Digital Currency - Information for crypto-asset users and tax professionals." Canada Revenue Agency, <https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency.html>.

³⁵⁰ Raiborn, C. and M. Sivitanides, "Accounting Issues Related to Bitcoins," *Journal of Corporate Accounting and Finance*, 26(2):25–34 (2015)

Regulators are deliberating on frameworks that strike a balance between fostering innovation in the DeFi sector and ensuring adequate tax compliance and are actively exploring strategies to grapple with the tax implications within the rapidly evolving DeFi space. Taxation, accounting, and regulatory frameworks may undergo changes contingent upon the classification of an entity as a currency, an asset (or investment), a commodity, or a digital service. The resolution of these complexities varies across countries, each at distinct stages of development and sophistication in addressing these issues.³⁵¹ Some scholars believe that tax authorities face an administrative hurdle when monitoring crypto transactions becomes excessively complex, primarily due to two inherent features of cryptocurrency: its volatile value and the anonymity associated with transactions. Overcoming this obstacle necessitates the adoption of advanced technologies to enforce tax regulations, alongside bolstering the reporting standards for crypto transactions³⁵².

A regulatory challenge emerges when the taxable foundation of a transaction becomes ambiguous due to the fluctuating value of cryptocurrencies and the anonymity inherent in these transactions. The volatility of cryptocurrency values complicates accurate tax reporting, as the value can change significantly between the time of transaction and reporting. Additionally, the anonymity associated with cryptocurrency transactions makes it difficult for tax authorities to identify the parties involved and enforce compliance³⁵³. To address these challenges, advanced technologies, such as blockchain analytics tools, can be employed to trace transactions and assess tax obligations accurately. Strengthening reporting requirements for crypto transactions can also improve transparency, ensuring that taxable events are properly recorded and reported.³⁵⁴ To meet the demands of DeFi and effectively regulate it, Canada must improve tax regulations by clarifying

³⁵¹ Brett Scott (2016) See note 61.

³⁵² Avi-Yonah, Reuven, and Mohanad Salaimi. "A New Framework for Taxing Cryptocurrencies." *The Tax Lawyer* 77, no. 1 (2023): 1-75. Accessed March 20, 2024.

https://dal.novanet.ca/permalink/01NOVA_DAL/ev10a8/cdi_proquest_journals_2930838638.

³⁵³ Ibid

³⁵⁴ Ibid

treatment, updating laws, collaborating with industry, implementing reporting requirements, and launching educational initiatives.

Chapter X: Environmental considerations of token mining and issuance.

As cryptocurrencies evolve as a financial market product, it is becoming increasingly clear that innovative solutions will be required to address significant upcoming challenges related to energy consumption and technological capacity³⁵⁵. Electricity consumption is a key factor in determining the value of mineable cryptocurrencies and plays a significant role in assessing their fair market value, which in turn impacts investment returns and should be integrated into trading strategies³⁵⁶. The distinction between mined and non-mined cryptos adds another layer of complexity. The mining process, prevalent in certain cryptocurrencies, introduces a unique aspect that may not align with the traditional characteristics of securities. As a result, attempting to regulate these assets solely under securities laws may not be suitable or effective. The energy demands of cryptocurrency mining have led to a considerable carbon footprint, now estimated to exceed that of several large industrial nations. Specifically, the process of validating and mining Bitcoin necessitates specialized hardware and substantial energy resources, contributing to ongoing carbon emissions³⁵⁷.

Additionally, the debate has become more complex as cryptocurrency supporters argue that the role of renewable energy in mining operations has been underestimated. While critics of the environmental impact estimates often highlight this oversight, it is likely that, given the limited use of renewable energy in countries with significant mining activities, the overall effect of cryptocurrency growth is increasing carbon emissions and harming the environment at its current rate of expansion³⁵⁸.

There are various digital currencies, with some being more energy-efficient than others. Corbet et al.³⁵⁹ classify digital assets into three categories: Currencies; Blockchains/Protocols;

³⁵⁵ Shaen Corbet, Andrew Urquhart & Larisa Yarovaya, *Cryptocurrency and Blockchain Technology* (Berlin: Walter de Gruyter GmbH, 2020) at ProQuest Ebook Central, online:

<http://ebookcentral.proquest.com/lib/dal/detail.action?docID=6305373>

³⁵⁶ Ibid

³⁵⁷ Ibid

³⁵⁸ Ibid

³⁵⁹ S Corbet, C Larkin, B Lucey, A Meegan & L Yarovaya, "Cryptocurrency Reaction to FOMC Announcements: Evidence of Heterogeneity Based on Blockchain Stack Position" (2020) 46:100706 *Journal of Financial Stability*.

DApps. This classification highlights that financial cryptocurrencies represent just one layer within the broader blockchain ecosystem. For digital currencies in the first category to have value, they must be scarce, a challenge that previous digital currencies faced. The mining process both creates and ensures this scarcity. Miners use computing power to solve mathematical problems, competing for a block reward (a Bitcoin payment to the first node to find the correct solution). This mining process is critical for generating value and scarcity in digital assets³⁶⁰.

Digital assets can be stored in various ways, including online wallets, online exchanges, hardware wallets, and paper wallets (cold storage). The environmental unsustainability of digital currencies primarily stems from the mining process.³⁶¹ In general, cryptocurrencies can be categorized into mineable and non-mineable currencies. In the following section the principles of Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA), with a particular focus on their respective environmental impacts is examined.

- Proof of Work (PoW)

The effectiveness of a decentralized blockchain network hinges significantly on the trustworthiness of its members. This assurance is upheld through the procedural framework, known as the consensus mechanism, employed by the network to oversee and authenticate transactions³⁶². Nakamoto (2008) claims to address the consensus problem in a permissionless blockchain by using an economic protocol called Proof-of-Work (PoW). PoW requires validators to compete in updating the blockchain by solving a simple puzzle, with success rates based solely on computational power³⁶³. Bitcoin's consensus mechanism, which minimizes the need for trust, is driven by its PoW algorithm. It is also one of the most famous cryptocurrencies that can be

³⁶⁰ Shaen Corbet, Andrew Urquhart & Larisa Yarovaya, (2020), see note 355

³⁶¹ Ibid.

³⁶² Iddo Bentov et al, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake" (2014) <https://eprint.iacr.org/2014/452.pdf>.

³⁶³ Nakamoto (2008), see note 28.

mined and traded today. This process requires machines to perform complex computations, leading to significant energy expenditures and rapidly increasing levels of energy consumption³⁶⁴.

In PoW, the next block in the blockchain is generated by the first miner to solve the algorithm correctly. Once a valid block is found, the miner broadcasts it to the network, where other miners verify its compliance with all rules and then abandon their own current efforts to work on this new block. The successful miner is compensated with a set amount of newly minted coins and the transaction fees from the transactions included in the block. This process repeats continuously, encouraging miners to keep mining Bitcoin. Due to the potential for substantial earnings, miners are motivated to operate energy-intensive machines to secure these rewards³⁶⁵. From an energy perspective, Bitcoin is a costly method of transaction, as participating in Bitcoin's validation and mining process necessitates specialized hardware and significant energy consumption. Consequently, this leads to both embedded carbon emissions and continuous carbon production. Currently, most mining pools consist of groups of miners operating in specialized warehouses equipped with large amounts of mining hardware. These networks predominantly rely on coal-fired power plants, leading to a significant carbon footprint for each transaction³⁶⁶.

- Proof of stake (PoS)

PoW was the pioneering consensus algorithm that demonstrated its viability, but it is not the sole method available. In recent years, in an effort to develop a sustainable permissionless blockchain that does not consume excessive energy, the blockchain community has explored more energy-efficient alternatives to PoW, such as Proof of Stake (PoS). Unlike proof-of-work, where miners use energy-intensive machines to generate numerous hashes per second, proof-of-stake allows coin owners to create blocks. This significantly reduces the energy consumption, making proof-of-stake a much more sustainable option compared to PoW³⁶⁷.

³⁶⁴ Fahad Saleh & Wei Jiang, "Blockchain without Waste: Proof-of-Stake" (2021) 34:3 Rev Fin Stud 1156 at 1156, online: <https://doi.org/10.1093/rfs/hhaa075>.

³⁶⁵ Shaen Corbet, Andrew Urquhart & Larisa Yarovaya, (2020), see note 355

³⁶⁶ Ibid

³⁶⁷ Ibid

PoS replaces the competitive nature of PoW by selecting a stakeholder at random to update the blockchain, and this algorithm employs validators who utilize staked coins to incorporate blocks into the blockchain³⁶⁸. This method eliminates the need for validators to engage in a costly computational competition. Despite this, there are concerns about the long-term effectiveness of PoS, as some believe it may not be able to achieve consensus³⁶⁹. Unlike PoW, which provides validators with a block reward for solving complex puzzles, PoS offers a similar monetary incentive for updating the blockchain without requiring validators to bear the significant financial costs associated with PoW³⁷⁰. It is worth to note that, on September 15, 2022, Ethereum, the second most valuable cryptocurrency and the pioneering smart contract blockchain, experienced a significant change. This upgrade shifted the network from the energy-demanding PoW system to the more environmentally sustainable PoS consensus model³⁷¹.

Besides energy efficiency, PoS enhances a network's resistance to fraud and theft³⁷². Validators, selected from network participants, are incentivized to act honestly to avoid losing their opportunity to earn rewards and suffering from inflation while others benefit. Additionally, malicious behavior risks their stake being slashed³⁷³. To launch an attack, an adversary would need to control most tokens in the network to alter consensus³⁷⁴. For instance, in a network of one hundred tokens, an attacker would need to acquire and stake fifty-one tokens to consistently approve and potentially modify transaction blocks. This creates a significant deterrent because attackers are financially invested in the network and would harm themselves by damaging the

³⁶⁸ Md. Mainul Islam, Mpyana Mwamba Merlec & Hoh Peter, "A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique," 2022 IEEE International Conference on Services Computing (SCC) (2022) 327 at 332, doi: 10.1109/SCC55611.2022.00054.

³⁶⁹ Fahad Saleh & Wei Jiang (2021), See note 364.

³⁷⁰ Ibid.

³⁷¹ Ethereum Foundation, "Proof-of-Stake (PoS)," online: Ethereum <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>.

³⁷² Jessica Hart, "Policing Proof-of-Stake Networks: Regulatory Challenges Presented by Staking-as-a-Service Providers and the Need for a Tailored Regime" (2022) 23:1 Columbia Sci & Tech L Rev 192, online: <https://doi.org/10.52214/stlr.v23i1.9392>.

³⁷³ Angela Angelovska-Wilson & Evan Weiss, "The Potential Legal Implications of Securing Proof of Stake-Based Networks" in Josias N Dewey et al, eds, *Blockchain & Cryptocurrency Regulation 2020*, 2nd ed (London: Global Legal Group, 2019) 133 at 134.

³⁷⁴ Ibid at 3.

economy³⁷⁵. Moreover, the cost and complexity of acquiring the necessary tokens would likely be prohibitive, with barriers including self-induced price inflation that could lead to the attacker's financial ruin³⁷⁶.

The accessibility of PoS networks to novice participants underlies their advantages in energy efficiency and security³⁷⁷. Since PoS does not require significant energy resources and offers enhanced safety, these networks are more accessible and appealing to individuals who lack the equipment needed for PoW mining³⁷⁸. This accessibility is one of PoS's most crucial and advantageous characteristics.

- Proof of authority (“PoA”)

PoA has gained popularity as a consensus algorithm for permissioned blockchains, where the network is managed by a set of trusted entities. This algorithm enables quick consensus and operates with lower computational and energy requirements³⁷⁹. PoA is a crash fault tolerance consensus algorithm that enhances the efficiency of private and consortium blockchains. Unlike PoW, it does not rely on the longest chain or confirmation rule. Instead, new blocks are added directly to the chain with unanimous approval from a group of trusted validators. Validators do not solve cryptographic puzzles, making this algorithm less demanding in terms of computing power³⁸⁰.

As the cryptocurrency industry expands and blockchain technology becomes more prevalent, it is crucial for cryptocurrencies to adopt more environmentally friendly blockchain solutions. By focusing on efficiency, these emerging cryptocurrencies can lower their environmental footprint. This trend demonstrates how enhancing an industry's environmental performance can be associated with increased productivity and effectiveness. Globally, coal and

³⁷⁵ Peercoin University, "Peercoin Proof-of-Stake Consensus", online: Peercoin <https://university.peercoin.net/#/9-peercoinproof-of-stake-consensus>.

³⁷⁶ Ibid.

³⁷⁷ Jessica Hart (2022), see note 372

³⁷⁸ Ibid

³⁷⁹ Md. Mainul Islam, Mpyana Mwamba Merlec & Hoh Peter (2022) See note 368.

³⁸⁰ Ibid.

other fossil fuels remain the dominant sources of electricity, significantly contributing to human-induced climate change³⁸¹. The combustion of coal releases carbon dioxide, a key driver of global warming. This dependence on fossil fuels has led to concerns that Bitcoin's energy consumption will rise as its popularity grows, raising important questions about the environmental sustainability of cryptocurrencies.

Evaluating the environmental impact of DeFi platforms is difficult due to the absence of standardized metrics. Regulators can also require DeFi platforms to transparently report their environmental metrics. Implementing uniform environmental reporting standards would allow regulators to effectively evaluate and compare the sustainability of various protocols³⁸². Mandating the disclosure of energy consumption, carbon emissions, and other relevant environmental data can help assess the sustainability of these platforms and encourage them to adopt greener practices. Governments and regulators are implementing mandatory environmental, social, and governance (“ESG”) disclosure requirements in regulated reports such as annual reports³⁸³. This initiative aims to educate investors on corporate ESG risks and opportunities, and to require entities to report on ESG factors affecting their financial performance, including the financial impacts of ESG-related risks and opportunities³⁸⁴. In the past, ESG reporting was optional and lacked uniformity, resulting in incomplete information and discontent among investors³⁸⁵. To remedy this, ESG reporting is now compulsory in numerous capital markets through regulatory filings. Nonetheless, global regulators are employing diverse strategies in enforcing ESG-specific financial reporting. Importantly, although some regulators or standard setters provide guidance tailored to specific industries, none have specifically assessed metrics that directly pertain to blockchain and other emerging technologies.³⁸⁶

³⁸¹ Shaen Corbet, Andrew Urquhart & Larisa Yarovaya, (2020), see note 355.

³⁸² Catherine Mulligan, Suzanne Morsfield & Evîn Cheikosman (2024), see note 79

³⁸³ Ibid

³⁸⁴ Ibid

³⁸⁵ Ibid

³⁸⁶ Ibid

Regulators must navigate the dual task of promoting innovation and technological progress in the DeFi sector while ensuring environmental sustainability. Achieving this balance necessitates the development of regulations that support energy-efficient consensus mechanisms and sustainable practices without hindering innovation. Providing regulatory incentives or rewards to platforms that adopt sustainable consensus mechanisms can promote environmentally friendly practices.

Chapter XI: Conclusion.

In the realm of DeFi regulation in Canada, lawmakers face a critical task of balancing innovation with the imperative of protecting users and maintaining the integrity of financial systems. Throughout this thesis, I have explored various regulatory challenges and proposed solutions, and it is important in this conclusion to draw connections back to the earlier sections to reinforce these ideas and highlight areas for future exploration. A comprehensive regulatory framework should prioritize several key considerations.

As outlined above, DeFi presents a new financial model that challenges existing regulatory frameworks, necessitating innovative approaches to regulation. This thesis further examined how DeFi differs from Fintech and cryptocurrencies, which are already beginning to be integrated into regulatory regimes. These differences highlight the need for tailored regulatory solutions, as traditional methods may not be applicable to decentralized systems.

The thesis further discussed the regulatory challenges that arise from DeFi's decentralized nature, such as the difficulty of assigning jurisdiction and the lack of centralized control. These challenges underscore the need for regulations that account for the unique characteristics of decentralized platforms, which I argued further in Section V regarding the potential for regulation in this space. The task of reconciling DeFi's decentralized nature with existing regulatory frameworks will require innovative approaches, particularly when it comes to crafting legal and regulatory language that is both accessible to humans and understandable by machines. This point links back to the discussion in Section VII on the need for clear legal definitions and standards, particularly regarding smart contracts.

The importance of standardization, which I introduced in Section VI, cannot be overstated. As I argued there, standardizing legal terminology and digital categorization—especially regarding smart contracts—will be crucial to ensuring consistent and effective regulation. This ties into Section VIII, where I explored the consumer protection implications of DeFi. Ensuring

transparency in smart contract terms, providing mechanisms for dispute resolution, and safeguarding users from risks will be essential to fostering trust in DeFi platforms. I also addressed security concerns, highlighting the need for stringent security standards to mitigate vulnerabilities in smart contracts. This point is further reinforced by my discussion on data privacy and cybersecurity, where I argued that protecting users' personal information should be a priority for regulators.

To address these regulatory challenges, Section VII also introduced the regulatory gaps in the oversight of stablecoins, macroprudential risks, and the need for banking-like safeguards, as well as the regulation of decentralized exchanges (DEXs) and virtual asset service providers (VASPs). Furthermore, I discussed the risks of fraud in DeFi and the legal safeguards needed to protect investors from fraudulent activities. Future research should explore these areas in more detail, particularly the implementation of investor protection measures and the development of effective fraud prevention mechanisms.

As the thesis progressed, I touched on the tax treatment of virtual assets, a critical aspect of regulatory compliance that must be balanced with the decentralized nature of DeFi. Similarly, the last section of the thesis addressed environmental concerns related to DeFi, such as the energy consumption of token mining and issuance. These environmental and tax issues demonstrate the broader impact of DeFi beyond traditional financial regulation, further emphasizing the need for a holistic regulatory framework.

In terms of future research, this thesis has laid the groundwork for a deeper exploration of how regulatory frameworks can evolve to accommodate the decentralized nature of DeFi. As discussed throughout the sections, key areas such as cross-border coordination, risk management practices, and educational initiatives require further investigation. Additionally, the balance between fostering innovation and ensuring regulatory oversight is an ongoing challenge that future work should continue to address.

It is important to note that this thesis does not delve into the role of DeFi in the monetary policy of central banks, an area ripe for future exploration. While this should not become the primary focus, the significant role that central banks have played in recent years in managing inflation, implementing quantitative tightening, and other monetary measures suggests that the interaction between DeFi and monetary policy deserves attention. Future research could explore whether DeFi offers an alternative to the inflationary and deflationary cycles associated with centralized currencies or how a growing reliance on DeFi might limit the ability of central banks to implement effective policy measures. This warrants further study, particularly in countries like Canada, where DeFi may increasingly impact the effectiveness of traditional monetary policy.

In conclusion, as I have argued throughout the thesis, a regulatory framework for DeFi in Canada must prioritize transparency, security, and consumer protection while remaining flexible enough to accommodate innovation. By addressing the regulatory challenges, including the standardization of legal language, the safeguarding of consumer data, and the regulation of smart contracts and decentralized exchanges, lawmakers can create an environment that supports the growth of DeFi while mitigating its risks. As I discussed in detail, concrete regulatory actions—such as enhancing scrutiny, increasing disclosure requirements, and promoting investor education—will be essential in achieving this balance. By fostering a regulatory environment that encourages innovation while ensuring the protection of users and the integrity of financial systems, Canada can lead the way in regulating DeFi and paving the path for future developments in this rapidly evolving space.

Security standards for smart contracts are imperative to mitigate vulnerabilities and ensure the integrity of transactions conducted through DeFi platforms. Similarly, regulations addressing data privacy concerns associated with smart contracts usage are necessary to protect users' personal information. Regulatory compliance must be upheld, balancing the unique characteristics of decentralized systems with existing financial regulations. Moreover, recognizing the decentralized

nature of governance in DeFi is crucial, urging exploration of regulatory approaches that respect and accommodate these structures. Robust risk management practices, cross-border coordination, educational initiatives, and clear regulatory frameworks are also essential components. Furthermore, advocating for an innovative yet flexible regulatory framework is key to encouraging DeFi growth while mitigating risks.

This imbalance could lead to increased risks of fraud and market manipulation, as seen in instances where regulatory oversight is lax, and fraudulent activities thrive under the guise of innovation. To address this imbalance, concrete regulatory actions should be implemented to shift the dial towards a more balanced approach. To address the imbalance between innovation and regulatory oversight, concrete actions are necessary. This may involve enhancing regulatory scrutiny and enforcement mechanisms, imposing stricter disclosure and reporting requirements, increased transparency measures, and more rigorous oversight of defi products and market participants and promoting investor education programs to empower individuals in making informed decisions.

In summary, by addressing these considerations and implementing concrete regulatory actions, lawmakers can foster a regulatory environment that supports the growth of DeFi and smart contracts in Canada while safeguarding users' interests and maintaining system integrity.

Reference list

Primary data

Alberta Securities Commission. Blanket Order 24-506, Exemption for Certain CTPS to be Recognized as Clearing Agencies. 29 August 2022.

Bill C-249 (44-1). An Act respecting the encouragement of the growth of the cryptoasset sector. Parliament of Canada. <https://www.parl.ca/legisinfo/en/bill/44-1/c-249>.

Budget Implementation Act, 2023, S.C. 2023, c. X (Can).

Canadian Payments Act. R.S.C. 1985, c. C-21

Canadian Securities Administrators. "Canadian Securities Regulators Expect Commitments from Crypto Trading Platforms Pursuing Registration." 15 August 2022. Canadian Securities Administrators. www.securities-administrators.ca/news/canadian-securities-regulators-expect-commitments-from-crypto-trading-platformspursuing-registration/.

Canadian Securities Administrators. "Crypto Trading Platforms Authorized to Do Business with Canadians." Accessed May 12, 2024. <https://www.securities-administrators.ca/crypto-trading-platforms-regulation-and-enforcement-actions/crypto-trading-platforms-authorized-to-do-business-with-canadians/>.

Canadian Securities Administrators. "CSA Staff Notice 21-332 Crypto Asset Trading Platforms: Pre-Registration Undertakings—Changes to Enhance Canadian Investor Protection" (February 22, 2023).

Canadian Securities Administrators. CSA Staff Notice 21-327. Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets. 16 January 2020. Online: Canadian Securities Administrators. <www.asc.ca/securities-law-and-policy/regulatory-instruments/21-327>

Canadian Securities Administrators. Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada. Consultation Paper 21-402, Proposed Framework For Crypto-Asset Trading Platforms. 14 March 2019. Online (PDF): Canadian Securities Administrators. <www.securities-administrators.ca/uploadedFiles/Industry_Resources/2019mars14-21-402-doc-cons-en.pdf>

Celsius Network LLC, Hoboken 22-10964 (Bankr D NY 13 July 2022).

Cred Inc, et al, Wilmington 20-12836 (Bankr D Del 09 November 2020).

Commodity Exchange Act, 7 USC § 1 (1936).

CSA Staff Notice 21-332. "Crypto Asset Trading Platform: Pre-Registration Undertakings - Changes to Enhance Canadian Investor Protection." 22 February 2023. OSC.

www.osc.ca/en/securities-law/instruments-rules-policies/2/21-332/csastaff-notice-21-332-crypto-asset-trading-platforms-pre-registration-undertakingschanges.

Canadian Securities Administrators, *National Instrument 45-106: Prospectus Exemptions* (2023).

CSA Staff Notice 46-307 Cryptocurrency Offerings. August 24, 2017.

https://www.osc.ca/sites/default/files/pdfs/irps/csa_20170824_cryptocurrency-offerings.pdf

CSA Staff Notice 46-308, "Securities Law Implications for Offerings of Tokens" (June 11, 2018). Ontario Securities Commission. Available online: <https://www.osc.ca/en/securities-law/instruments-rules-policies/4/46-308/csa-staff-notice-46-308-securities-law-implications-offerings-tokens> [accessed on February 8, 2024].

Currency Act, R.S.C. 1985, c. C-52.

Exchange Act Release No. 15769 (April 26, 1979), 44 FR 26688

Excise Tax Act, RSC 1985, c E-15, <https://laws-lois.justice.gc.ca/eng/acts/e-15/>.

FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021. Online: FATF <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf>.

Income Tax Act, RSC 1985, c. 1 (5th Supp).

Jenson v. Continental Financial Corporation, 404 F.Supp. 792 (D.C. Minn. 4th Div., 1975).

Joint Canadian Securities Administrators, Investment Industry Regulatory Organization of Canada. "Staff Notice 21-330 - Guidance for Crypto-Trading Platforms: Requirements relating to Advertising, Marketing and Social Media Use." 23 September 2021. Canadian Securities Administrators. www.asc.ca/securities-law-andpolicy/regulatory-instruments/21-330.

Joint CSA-IIROC Staff Notice 21-329. "Joint CSA-IIROC Staff Notice 21-329."

National Instrument 31-103, Companion Policy on Registration Requirements, Exemptions and Ongoing Registrant Obligations.

Office of the Superintendent of Financial Institutions. "Interim Arrangements for the Regulatory Capital and Liquidity Treatment of Crypto Asset Exposures." 18 August 2022. Online. OSFI. <www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/crypto22.aspx>.

Ontario Securities Commission. "OSC Highlights Potential Securities Law Requirements for Businesses." Press Release. 8 March 2017. Ontario Securities Commission.

<https://www.osc.ca/en/news-events/news/osc-highlights-potential-securities-law-requirements-businesses>.

Ontario Securities Commission. "OSC Holds Global Crypto Asset Trading Platforms Accountable." 22 June 2022. OSC. www.osc.ca/en/news-events/news/osc-holds-global-crypto-asset-trading-platforms-accountable.

Ontario Securities Commission. "QuadrigaCX: A Review by Staff of the Ontario Securities Commission." 14 April 2020. Online: OSC. <www.osc.ca/quadrigacxreport/>

Ontario Securities Commission. "Registered Crypto Asset Trading Platforms." Online: OSC. <www.osc.ca/en/industry/registration-and-compliance/registered-crypto-asset-trading-platforms>. Last accessed 6 January 2023

Ontario Securities Commission. CSA Multilateral Notice of Multilateral Instrument 91-102, Prohibition of Binary Options and Related Companion Policy. 28 September 2017. Online. OSC. <www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170927_91-102_binaryoptions.htm>.

Ontario Securities Commission. In The Matter Of Coinsquare Ltd., Cole Diamond, Virgile Rostand And Felix Mazer, Settlement Agreement. 16 July 2020.

Ontario Securities Commission. In The Matter Of Coinsquare Ltd., Cole Diamond, Virgile Rostand And Felix Mazer, Settlement Agreement. 16 July 2020. [OSC, Settlement Agreement with Coinsquare Ltd.].

Ontario Securities Commission. Statement of Allegations, Bybit Fintech Limited (Bybit). 21 June 2021.

Ontario Securities Commission. Statement of Allegations, Mek Global Limited and PhoenixFin Pte Ltd (collectively KuCoin). 2 June 2021.

Ontario Securities Commission. Statement of Allegations, Polo Digital Assets, Ltd (Poloniex). 25 May 2021.

Pacific Coast Coin Exchange of Canada v. Ontario (Securities Commission), 1977 CarswellOnt 50.

Pacific Coast Coin Exchange v. Ontario (Securities Commission), [1978] 2 SCR 112.

Payment Clearing and Settlement Act. S.C. 1996, [PCSA].

Payment Services Act 2019 (Singapore), Cap. 222A (2019 Rev. Ed.), available online: <https://sso.agc.gov.sg/Act/PSA2019>.

Quadriga Fintech Solutions Corp, Whiteside Capital Corporation & 0984750 BC Ltd (1 April 2019), Halifax 484742 (NS SC), Termination and Bankruptcy Assignment Order.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. Online: EUR-Lex. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>.

Re Shelter Corporation of Canada Ltd., 1977 O.S.C.B. 6.

SEC v WJ Howey Co, 328 US 293 (1946).

Securities Act, R.S.A. 2000, c. S-4, s.1.

Securities Act, R.S.B.C. 1996, c. 418, s.1(1).

Securities Act, R.S.O. 1990, c. S.5, s. 1.1.

Securities and Futures Act 2001 (Singapore), Rev. Ed. Cap. 289 (2006 Reprint), available online: <https://sso.agc.gov.sg/Act/SFA2001>.

See Office of the Superintendent of Financial Institutions, "Interim Arrangements for the Regulatory Capital and Liquidity Treatment of Crypto Asset Exposures" (18 August 2022), online: OSFI <www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/crypto22.aspx

Teksavvy Solutions Inc. v. Bell Media Inc. (2021) 2021 CAF 100, 2021 FCA 100

Terraform labs Pte Ltd (Terra Luna) (23 September 2022), Singapore HC/OC 247/2022 (SGHC [Gen Div]).

Three Arrows Capital Ltd, New York 1:22-bk-10920 (Bankr D NY 01 July 2022).

U.S. Securities and Exchange Commission. Press Release, "SEC Charges Caroline Ellison and Gary Wang with Defrauding Investors in Crypto Asset Trading Platform FTX." 21 December 2022. SEC. www.sec.gov/news/press-release/2022-234.

Tully, Shawn. "Is this a Bitcoin bubble? The debate is roiling some of Wall Street's most seasoned investors" *Fortune* (21 October 2021) online: <https://fortune.com/2021/10/21/is-this-a-bitcoin-bubble-the-debate-is-roiling-some-of-wall-streets-most-seasoned-investors/>.

U.S. Securities and Exchange Commission. Press Release, "SEC Charges Nishad Singh with Defrauding Investors in Crypto Asset Trading Platform FTX." 28 February 2023. SEC. www.sec.gov/news/press-release/2023-40.

U.S. Securities and Exchange Commission. Press Release, "SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX." 13 December 2022. SEC. www.sec.gov/news/press-release/2022-219.

Uniform Regulation of Virtual Currency Businesses Act, s 23, online: <https://www.cga.ct.gov/2018/TOB/h/2018HB-05496-R00-HB.htm> (accessed on January 25, 2024). Raised Bill No. 5496, February Session, 2018, LCO No. 2228.

United States Department of Justice. Press Release, "United States Attorney Announces Charges Against FTX Founder Samuel Bankman-Fried." 13 December 2022. Department of Justice. www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried.

Voyager Digital Holdings, Inc, New York 22-10943 (Bankr D NY 05 July 2022).

Williamson, Re, 1993 CarswellOnt 1523, 16 O.S.C.B. 2689 (Ont. Securities Comm.).

Secondary data

"Forex goes into future shock." Euromoney, October 2001. <https://people.duke.edu/~charvey/Media/2001/EuromoneyOct01.pdf>.

Agarwal, Udit, Vinay Rishiwal, Sudeep Tanwar, and Mano Yadav. "Blockchain and crypto forensics: Investigating crypto frauds." *International Journal of Network Management* (2023): e2255. DOI: 10.1002.

Aiello, Rachel. "Conservative MP's Bill to Encourage Growth in Cryptocurrency Sector Defeated." CTV News, November 23, 2022. <https://www.ctvnews.ca/politics/conservative-mp-s-bill-to-encourage-growth-in-cryptocurrency-sector-defeated-1.6165880>.

Alex Lipton, Stuart Levi, Skadden. "An Introduction to Smart Contracts and Their Potential and Inherent Limitations." Harvard Law School Forum on Corporate Governance (May 26, 2018)

Allen, Hilary J. *Driverless Finance: Fintech's Impact on Financial Stability*. Oxford: Oxford University Press, 2022.

Ammous, Saifedean. "Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation, and International Development." *The Journal of Private Enterprise* 3 (2015).

Angela Angelovska-Wilson & Evan Weiss, "The Potential Legal Implications of Securing Proof of Stake-Based Networks" in Josias N Dewey et al, eds, *Blockchain & Cryptocurrency Regulation 2020*, 2nd ed (London: Global Legal Group, 2019) 133.

Aramonte, Sirio et al. "DeFi Risks and the Decentralization Illusion." *BIS Quarterly Review*, no. 27 (December 2021): 27.

Arner, Douglas, Auer, Raphael, & Frost, Jon. "Stablecoins: risks, potential and regulation." *BIS Working Papers*, No. 905, Monetary and Economic Department, November 2020. <https://www.bis.org/publ/work905.pdf>.

Arslanian, Henri. "The History of Money." In *The Book of Crypto*, 1–43. Cham: Palgrave Macmillan, 2022. Online: https://doi.org/10.1007/978-3-030-97951-5_22.

Auer, R., & Böhme, R. "The Technology of Retail Central Bank Digital Currency." *BIS Quarterly Review* (March 2020) 85 at 100.

Auer, R., & Böhme, R. *The Technology of Retail Central Bank Digital Currency*. *BIS Quarterly Review*, March 2020, pp. 85-100.

Auer, Raphael, Jon Frost, & Jose Maria Vidal Pastor. "Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi." 16 June 2022. Online. *BIS Bulletin No. 58*. <www.bis.org/publ/bisbull58.htm>.

Auer, Raphael Anton. *Embedded Supervision: How to Build Regulation into Decentralised Finance*. St. Louis: CESifo, 2022. ProQuest. Online: <https://ezproxy.library.dal.ca/login?url=https://www.proquest.com/working-papers/embedded-supervision-how-build-regulation-into/docview/2675434688/se-2>.

Avi-Yonah, Reuven, and Mohanad Salaimi. "A New Framework for Taxing Cryptocurrencies." *The Tax Lawyer* 77, no. 1 (2023): 1-75. Accessed March 20, 2024. https://dal.novanet.ca/permalink/01NOVA_DAL/ev10a8/cdi_proquest_journals_2930838638.

Azman, Mohamed, and Kunal Sharma. "HCH DEX: A Secure Cryptocurrency e-Wallet & Exchange System with Two-way Authentication." In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 305-310. Tirunelveli, India: IEEE, 2020. doi: 10.1109/ICSSIT48917.2020.9214122.

Back, Adam. "Hashcash-A Denial of Service Counter-Measure" (1st August 2002). Online: <http://www.hashcash.org/papers/hashcash.pdf>.

Bambrough, Billy. "New Research Reveals 'Systemic Risk' To Bitcoin As Its Price Crashes Under \$60,000." 27 October 2021. Online. *Forbes*. <www.forbes.com/sites/billybambrough/2021/10/27/new-research-reveals-systemic-risk-to-bitcoin-as-its-price-crashes-under-60000/?sh=51530373e066>.

Bank for International Settlements. "Central Bank Digital Currencies: Foundational Principles and Core Features." 9 October 2020. Online. *BIS*. <www.bis.org/publ/othp33.htm>.

Bank of Canada. "Contingency Planning for a Central Bank Digital Currency." 25 February 2020. Online. *Bank of Canada*. <www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/>.

Bank of Canada. "Money and Payments in the Digital Age, Remarks by Timothy Lane, Deputy Governor, CFA Montreal Fintech RDV2020." February 2020. Online PDF. *Bank of Canada*. <www.bankofcanada.ca/wp-content/uploads/2020/02/remarks-250220.pdf>.

Bank of Canada. "Potential benefits and key risks of fiat-referenced cryptoassets." Staff Analytical Note 2022-20. Hugh Ding, Natasha Khan, Bena Lands, Cameron MacDonald, Laura Zhao. December 2022. <https://www.bankofcanada.ca/2022/12/staff-analytical-note-2022-20/>.

Bank of Canada. "The Positive Case for a CBDC." 20 July 2021. Staff Discussion Paper 2021-11. Bank of Canada.

Barsan, Iris M. "Legal Challenges of Initial Coin Offerings." 2017 *Revue Trimestrielle de Droit Financier* 54 (2017): 56-60.

Basic Attention Token. Online: <https://basicattentiontoken.org/>.

Bentov, Iddo et al, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake" (2014), <https://eprint.iacr.org/2014/452.pdf>.

BGIN (Blockchain Governance Initiative Network). (2021). "Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations", BGIN SR 001.

Bodkhe, U., Tanwar, S., Bhattacharya, P., & Kumar, N. (2022). Blockchain for precision irrigation: opportunities and challenges. *Transactions on Emerging Telecommunications Technologies*, 33(10), e4059

Bonini, S., Capizzi, V. & Zocchi, P. "The Performance of Angel-Backed Companies" (2019) 100 *Journal of Banking & Finance* 328-345.

Braun, Helene. "Binance Controlled 92% of Bitcoin Spot Trading Volume at End of 2022: Arcane Research." 4 January 2023. Online. CoinDesk. <www.coindesk.com/markets/2023/01/04/binance-controlled-92-of-bitcoin-spot-trading-volume-at-end-of-2022-arcane-research/>.

Brownell, Claire. "With Crypto-Staking Approvals, Canada's Securities Regulators Mark Another World First." 17 November 2022. (Online) The Logic. <theologic.co/news/with-crypto-staking-approvals-canadas-securities-regulators-mark-another-worldfirst/>.

Brummer, Chris. "Disclosure, DApps and DeFi." (2022) 5:2 *Stanford Journal of Blockchain Law & Policy*, 137-174. Available at: <https://assets.pubpub.org/efeeza8o/01656289809141.pdf>.

Businesswire. *Coinfirm Releases Smart Contract AML Oracle For DeFi Compliance*. 5 May 2022. Online: Businesswire <https://www.businesswire.com/news/home/20220505006077/en/Coinfirm-Releases-Smart-Contract-AML-Oracle-For-DeFi-Compliance>.

Butenko, Anna, and Pierre Larouche. "Regulation for Innovativeness or Regulation of Innovation?" *Law, Innovation and Technology* 7, no. 1 (2015): 52-82. <https://doi.org/10.1080/17579961.2015.1052643>.

Buterin, Vitalik. "A Next Generation Smart Contract & Decentralized Application Platform." Ethereum White Paper. 2013.

Butler, T., Al Khalil, F., O'Brien, L., & Ceci, M. (2017). "Smart Contracts and Distributed Ledger Technologies in Financial Services: Keeping Lawyers in the Loop." 36(9) Banking & Financial Services Policy Report, 1-11.

Cahill, John, Jana S. Farmer & William H. Behr. "First DOJ NFT Insider Trading Charges Mark New Enforcement Era." 29 June 2022. Online. Bloomberg Law. <news.bloomberglaw.com/us-law-week/first-doj-nft-insider-trading-charges-marks-new-enforcement-era-16>.

Catalini, Christian, and Alonso de Gortari. "On the Economic Design of Stablecoins." (5 August 2021). Available online: SSRN <https://ssrn.com/abstract=3899499>.

Catherine Mulligan, Suzanne Morsfield & Evîn Cheikosman. "Blockchain for sustainability: A systematic literature review for policy impact." (2024) 48:2 Telecommunications Policy 102676, online: ScienceDirect <https://doi.org/10.1016/j.telpol.2023.102676>.

Chainlink, "*LINK Token Contracts*": <https://docs.chain.link/resources/link-token-contracts>.

Chiu, Jonathan, and Hanna Yu. "Regulatory concerns for decentralized finance." Staff Analytical Note 2023-15. Bank of Canada, October 2023. Accessed February 14, 2024. URL: <https://www.bankofcanada.ca/2023/10/staff-analytical-note-2023-15/>

Chiu, Jonathan & Yu, Hanna. "Decentralized Finance: Innovations and Challenges." Bank of Canada Staff Analytical Note 2023-15 (English). October 2023. [Online] Available at: <https://www.bankofcanada.ca/2023/10/staff-analytical-note-2023-15/>

Christian Catalini & Jai Massari, "Stablecoins and the Future of Money," Harvard Business Review (August 10, 2021), <https://hbr.org/2021/08/stablecoins-and-the-future-of-money>.

Clements, Ryan, and Virginia Torrie. "Crypto Asset Regulation in Canada: Developments and Governance Considerations." Banking & Finance Law Review 39, no. 3 (2023): 345-380.

Clements, Ryan. "Built to Fail: The Inherent Fragility of Algorithmic Stablecoins." (2021) 11 Wake Forest L. Rev. Online 131. Wake Forest Law Review. www.wakeforestlawreview.com/2021/10/built-to-fail-the-inherent-fragility-of-algorithmic-stablecoins/.

Clements, Ryan. "Defining the Regulatory Perimeter for Stablecoins in Canada." (2022) 66 Can. Bus. L. J. 201.

Clements, Ryan. "Emerging Canadian Crypto-Asset Jurisdictional Uncertainties and Regulatory Gaps." Banking & Finance Law Review 37, no. 1 (2021)

Cohen, Lewis, Angela Angelovska-Wilson, & Greg Strong. "Decentralized Finance: Have Digital Assets and Open Blockchain Networks Found Their 'Killer App'?" (2021) Global Legal Insights, Blockchain & Cryptocurrency Regulation.

Corbet, S, C Larkin, B Lucey, A Meegan & L Yarovaya. "Cryptocurrency Reaction to FOMC Announcements: Evidence of Heterogeneity Based on Blockchain Stack Position." (2020) 46:100706 Journal of Financial Stability.

Corbet, Shaen, Andrew Urquhart & Larisa Yarovaya. *Cryptocurrency and Blockchain Technology*. Berlin: Walter de Gruyter GmbH, 2020. At ProQuest Ebook Central, online: <http://ebookcentral.proquest.com/lib/dal/detail.action?docID=6305373>

Corbet, Shaen et al. *Cryptocurrency and Blockchain Technology*. Berlin: Walter de Gruyter GmbH, 2020. At ProQuest Ebook Central, online: <http://ebookcentral.proquest.com/lib/dal/detail.action?docID=6305373> [created from dal on 2024-05-21].

Corbet, Shaen, ed. *Understanding Cryptocurrency Fraud: The Challenges and Headwinds to Regulate Digital Currencies*. Berlin: De Gruyter, 2022. Online: <https://doi.org/10.1515/9783110718485>.

Crafts, Nicholas. "Regulation and Productivity Performance." *Oxford Review of Economic Policy* 22, no. 2 (Summer 2006): 186–202. <https://doi.org/10.1093/oxrep/grj012>.

Crenshaw, C.A. (SEC Commissioner). "Statement on DeFi Risks, Regulations, and Opportunities." The United States Securities and Exchange Commission (2021).

Cumming, Douglas J., Sofia Johan, and Anshum Pant. "Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty." *Journal of Risk and Financial Management* 12, no. 3 (2019): 126. DOI: 10.3390/jrfm12030126

Cumming, Douglas J., Sofia Johan, and Anshum Pant. "Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty." *Journal of Risk and Financial Management* 12, no. 3 (2019): 126. DOI: 10.3390/jrfm12030126.

Cunliffe, Jon. "Is 'Crypto' a Financial Stability Risk?" Speech delivered at Bank of England, London, 13 October 2022. Online. Bank of England. <www.bankofengland.co.uk/speech/2021/october/jon-cunliffe-swifts-sibos-2021>.

Deshant Singh Thakur, Raj A Varma & Damodar Mayappa Hake, "Regulation of Cryptocurrency in India: Issues and Challenges" (2022) 6:5 Journal of Positive School Psychol, online: <https://journalppw.com/index.php/jpsp/article/view/9707/6356>.

Digital Assets. "Crypto Market Insights: 3 Key Differences Between DeFi and Centralized Finance Platforms" (15 May 2023), online: Forbes <https://www.forbes.com/sites/digital->

[assets/2023/05/15/crypto-market-insights-3-key-differences-between-defi-and-centralized-finance-platforms/](https://assets.2023/05/15/crypto-market-insights-3-key-differences-between-defi-and-centralized-finance-platforms/).

Dierksmeier, C., & Steele, P. (2016). "Cryptocurrencies and Business Ethics." *Journal of Business Ethics*, 1–14. <https://doi.org/10.1007/s10551-016-3298-0>.

Douglas Arner, Raphael Auer, and Jon Frost. "Stablecoins: Risks, Potential and Regulation." Bank for International Settlements Working Paper No. 905.

Ethereum Explanatory Document, Introduction to Dapps." ETHEREUM. <https://ethereum.org/en/developers/docs/dapps>

Ethereum Foundation, "Proof-of-Stake (PoS)," online: Ethereum <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> (last edited 29 March 2024).

Expert Group on Regulatory Obstacles to Financial Innovation. "Final Report: 30 Recommendations on Regulation, Innovation, and Finance." European Commission, Brussels, Belgium, December 13, 2019. https://finance.ec.europa.eu/system/files/2019-12/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf.

Fahad Saleh & Wei Jiang, "Blockchain without Waste: Proof-of-Stake" (2021) 34:3 Rev Fin Stud 1156, online: <https://doi.org/10.1093/rfs/hhaa075>.

Financial Conduct Authority, Bank of England. "Digital Regulatory Reporting: Pilot 1 Phase Report." 13 March 2019. Online: <https://www.fca.org.uk/publication/discussion/digital-regulatory-reporting-pilot-phase-1-report.pdf>.

Financial Stability Board. "Review of the FSB High-Level Recommendations of the Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements: Consultative Report." Basel: FSB, October 11, 2022.

Financial Times. "Can Crypto Contagion Infect Mainstream Finance?" 30 June 2022. Online. FT. <www.ft.com/content/03bb9296-b645-4311-abb2-14bc3ab66443>.

Francus, Lily. "Block by Block: Assessing Risk in Decentralized Finance." Moody's Analytics: Credit Where Due Blog Series (January 2022). Available at https://www.moodyanalytics.com/articles/2021/block_by_block_assessing_risk_in_decentralized_finance.

Frost, J., Shin, H. S., & Wierds, P. "An Early Stablecoin? The Bank of Amsterdam and the Governance of Money." BIS Working Papers No 902 (2020).

Frost, J., Shin, H. S., & Wierds, P. *An Early Stablecoin? The Bank of Amsterdam and the Governance of Money*. BIS Working Papers No 902, 2020.

Frost, Jon, Hyun Song Shin, and Peter Wierts. "An early stablecoin? The Bank of Amsterdam and the governance of money." BIS Working Papers, No. 902, November 10, 2020. <https://www.bis.org/publ/work902.pdf>.

G7 Working Group on Stablecoins. "Investing the Impact of Global Stablecoins." Bank for International Settlements, Committee on Payments and Market Infrastructures. October 2019. www.bis.org/cpmi/publ/d187.pdf.

Geva, Benjamin. 'Cryptocurrencies and the Evolution of Banking, Money, and Payments.' In *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*, edited by C. Brummer. Oxford: Oxford University Press, 2019. 20-22.

Geva, Benjamin. 'Cryptocurrencies and the Evolution of Banking, Money, and Payments.' In *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*, edited by C. Brummer. Oxford: Oxford University Press, 2019. 20-22.

Geva, Benjamin. "Cryptocurrencies and the Evolution of Banking, Money and Payments." In *Cryptoassets: Legal, Regulatory and Monetary Perspectives*, edited by Chris Brummer, 11-38. Oxford University Press, 2019.

Gimigliano, Gabriella. "Payment Tokens and the Path Towards MiCA." *The Italian Law Journal* 8, no. 1 (2021): 381. Online: <https://usiena-air.unisi.it/retrieve/1c80bed0-a603-494c-818b-a63c2b4dfed8/gimigliano%20TILJ.pdf>

Gogel, David et al. "DeFi Beyond the Hype: The Emerging World of Decentralized Finance." Wharton Blockchain & Digital Asset Project, Wharton School, University of Pennsylvania (2021). Online PDF. WIFPR. <wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf>.

Government of Canada. "Cryptocurrency Guide." Canada Revenue Agency. <https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html>.

Haber, S., & Stornetta, W.S. "How to time-stamp a digital document." *Journal of Cryptology* 3, no. 2 (1991): 99-111.

Hacker, Philipp & Thomale, Chris. "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law." Last revised May 2, 2018. Pages 33–37. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=30758

Hart, Jessica. "Policing Proof-of-Stake Networks: Regulatory Challenges Presented by Staking-as-a-Service Providers and the Need for a Tailored Regime" (2022) 23:1 *The Columbia Science and Technology Law Review* 192. Online: <https://doi.org/10.52214/stlr.v23i1.9392>.

Harvey, Campbell R., Ashwin Ramachandran, and Joey Santoro. *DeFi and the Future of Finance*. April 5, 2021. <https://compoundmaven.com/wp-content/uploads/2022/08/DeFi-And-The-Future-Of-Finance-Duke-University-August-2021.pdf>.

Harvey, Campbell R. "The History of Digital Money" (2020). Online: https://faculty.fuqua.duke.edu/~charvey/Teaching/697_2020/Public_Presentations_697/History_of_Digital_Money_2020_697.pdf.

Holtmeier, Moritz, and Philipp Sandner. "*The Impact of Cryptocurrencies on Developing Countries*." Frankfurt School Blockchain Centre Working Paper, December 2019.

Hong Kong Institute for Monetary and Financial Research. *Decentralised Finance: Current Landscape and Regulatory Developments*. June 2024. HKIMR Applied Research Report No 1/2024. Online: <https://www.aof.org.hk/docs/default-source/hkimr/applied-research-report/defirep.pdf>.

Houben, R. and Snyers, A. 'Cryptoassets: Key Elements, Regulatory Concerns and Responses.' Study requested by the ECON Committee of the European Parliament (2020).

Huyghebaert, N. "The Capital Structure of Business Start-Ups: Policy Implications" (2003) 48:1 *Tijdschrift voor Economie en Management*, online: <https://lirias.kuleuven.be/retrieve/12808>.

International Monetary Fund. "The Crypto Ecosystem and Financial Stability Challenges." October 2021. Online. IMF. <www.imf.org/-/media/Files/Publications/GFSR/2021/October/English/ch2.ashx>.

Jaag, Christian, and Bach, Christian. "Cryptocurrencies: New Opportunities for Postal Financial Services." Working Papers 0052, Swiss Economics, 2015.

James Angel & Ryosuke Ushida, "Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs" in FC 2021 International Workshops, in Matthew Bernhard et al., eds., *Financial Cryptography and Data Security FC 2021 International Workshops* (Berlin: Springer, 2021) 21 at 33.

Jarno, Klaudia & Kołodziejczyk, Hanna. "Does the Design of Stablecoins Impact Their Volatility?" (2021) 14(2) *Journal of Risk Financial Management* 42. <https://doi.org/10.3390/jrfm14020042>.

Jensen, Johannes R., Victor von Wachter, & Omri Ross. "An Introduction to Decentralized Finance (DeFi)" (2021) 26 *Complex Systems Informatic & Modeling Quarterly* 46.

Jiahua Xu & Yebo Feng, "Reap the Harvest on Blockchain: A Survey of Yield Farming Protocols," in (2023) 20:1 *IEEE Transactions on Network and Service Management* 858 at 869, doi: 10.1109/TNSM.2022.3222815.

Kharif, Olga. "Bitcoin Whales' Ownership Concentration is Rising During Rally." 18 November 2020. Online. BNN Bloomberg. <www.bnnbloomberg.ca/bitcoin-whales-ownership-concentration-is-rising-during-rally-1.1524504>.

Klöhn, Lars et al. "Initial Coin Offerings (ICOs)." 30 *Zeitschrift für Bankrecht und Bankwirtschaft* 89 (2018): 99.

Kozhan, Roman & Viswanath-Natraj, Ganesh. "Decentralized Stablecoins and Collateral Risk" (1 September 2021), online (pdf): https://acfr.aut.ac.nz/_data/assets/pdf_file/0004/570307/DAI_Paper_SSRNSeptember2021.pdf.

Lagarde, Christine (ed). *Winds of Change: The Case for New Digital Currency*. International Monetary Fund, 2018.

Lu, Shaofei et al. "CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle." (2023) 23:4 *Sensors* 1864. Online: <https://doi.org/10.3390/s23041864>.

Campbell-Verduyn, Malcolm, ed, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, 1st ed, RIPE Series in Global Political Economy (London: Routledge, 2017), online: <https://doi.org/10.4324/9781315211909>.

MacNaughton, Alan, Kevin Milligan, Daniel Sandler, and Frances Woolley. "Policy Forum: Editors' Introduction - The Tax Treatment of Cryptoassets." *Canadian Tax Journal* 71, no. 1 (2023): 33-37.

Mancini-Griffoli, Tommaso, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu & Celine Rochon, *Casting Light on Central Bank Digital Currency* (November 2018), IMF Staff Discussion Note SDN/18/08, online: IMF <https://www.imf.org/-/media/Files/Publications/SDN/2018/SDN1808.ash>.

Marian, Omri. "Are Cryptocurrencies Super Tax Havens?" *Michigan Law Review* 112, no. 1 (2013): 42–3.

Marty, Frédéric, and Thierry Warin. Visa's Abandoned Plan to Acquire Plaid: What Could Have Been a Textbook Case of a Killer Acquisition. CIRANO Scientific Paper No 2021S-39. Available online: <https://cirano.qc.ca/files/publications/2021s-39.pdf>.

Massad, Timothy G. "Facebook's Libra 2.0: Why You Might Like It Even if We Can't Trust Facebook." June 2020. Online (PDF). Economic Studies at Brookings. <www.brookings.edu/wp-content/uploads/2020/06/ES-6.22.20-Massad-1.pdf>.

Maume, Philipp & Fromberger, Mathias. "Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws." (2019) 19:2 *The Chicago Journal of International Law* (accessed on May 8, 2024). Available at: <https://cjl.uchicago.edu/print-archive/regulation-initial-coin-offerings-reconciling-us-and-eu-securities-laws>.

Md. Mainul Islam, Mpyana Mwamba Merlec & Hoh Peter, "A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique," 2022 IEEE International Conference on Services Computing (SCC) (2022) 327-332, doi: 10.1109/SCC55611.2022.00054.

Mills, D., Wang, K., Malone, B., et al. "Distributed Ledger Technology in Payments, Clearing, and Settlement." Federal Reserve Board Finance and Economics Discussion Series, no 2016-095, December 2016, 17. www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

Nabilou, Hossein. 'Bitcoin Governance as a Decentralized Financial Market Infrastructure.' (2020) 4(2) Stanford Journal of Blockchain Law and Policy 177-202.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org, 2009. <https://bitcoin.org/bitcoin.pdf>.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008). Online: <<https://bitcoin.org/bitcoin.pdf>>

Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu & Adefolake Olachi Adewusi, "International Enforcement of Cryptocurrency Laws: Jurisdictional Challenges and Collaborative Solutions" (2024) 11:2 Magna Sci Adv Res Rev, online: <https://doi.org/10.30574/msarr.2024.11.1.0075>.

Nicholls, Christopher C. *Securities Law*. 3rd ed. Toronto: Irwin Law Inc, 2023.

Omarova, Saule T. "New Tech v. New Deal: Fintech as a Systemic Phenomenon." (2019) 36(2) Yale Journal on Regulation 36.

Ontario Securities Commission. "OSC Holds Global Crypto Asset Trading Platforms Accountable." 22 June 2022. Online. OSC. <www.osc.ca/en/news-events/news/oscholds-global-crypto-asset-trading-platforms-accountable>

Ortolani, Pietro. "Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin." *Oxford Journal of Legal Studies* 36, no. 3 (Autumn 2016): 595-629. Oxford University Press.

Peercoin University. "Peercoin Proof-of-Stake Consensus". Online: Peercoin <https://university.peercoin.net/#/9-peercoinproof-of-stake-consensus>.

Peng, Mike W et al. "An Institution-Based View of Global IPR History" (2017) 48:7 Journal of International Business Studies 893-907, online: https://ideas.repec.org/a/pal/jintbs/v48y2017i7d10.1057_s41267-016-0061-9.html.

Rohr, Jonathan & Wright, Aaron. "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets." U. Tenn. Legal Stud. Res. Paper No. 338, Cardozo Legal Stud. Res. Paper No. 527 (2018): 14–26.

Reuters, "Chinese Financial, Payment Bodies Barred from Cryptocurrency Business" (18 May 2021), online: <https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/>.

Sanz-Bas, David, Carlos del Rosal, Sergio Luis Nández Alonso & Miguel Ángel Echarte Fernández. "Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain" (2021) 10:3 *Laws* 57, online: <https://doi.org/10.3390/laws10030057>.

Schär, Fabian. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." 15 April 2021. 103(2) *Review of Economic Research*, Federal Reserve Bank of St. Louis. Online. St. Louis Fed. <research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets>.

Scott, Brett. "How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?" UNRISD Working Paper No. 2016-1. United Nations Research Institute for Social Development, Geneva, 2016.

Spulber, Daniel F. "Unlocking Technology: Antitrust and Innovation." *Journal of Competition Law* 4 (2008): 915–66.

Susan Athey, "5 Ways Digital Currency Will Change the World," *World Economic Forum Agenda* (Jan. 22, 2015).

S S, AR Saxena, YR Saxena, MSM Sana, S Verma & S Roy. "Decentralized Finance and Cross-Chain Interoperable Automated Market Maker - Using BlockChain." In 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), Vellore, India, 2024, 1-9. DOI: 10.1109/ic-ETITE58242.2024.10493513.

Tapscott, Don & Tapscott, Alex. *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (May 2016) at 72, 83, 101, 127.

The Board of the International Organization of Securities Commissions. "Global Stablecoin Initiatives." Public Report, OR01/2020, March 2020. <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf>.

The U.S. Commodity Futures Trading Commission (CFTC). "Customer Advisory: Beware Virtual Currency Pump-and-Dump Schemes." https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_pumpedump0218.pdf.

Tinianow, Andrea & Palley, Stephen. "A Round Table Discussion on Stablecoins: Taking the World By Storm or Storming the World?" (2022) 3 *International Journal of Blockchain Law* 4.

Tomizawa, Aki et al. "Economic Growth, Innovation, Institutions, and the Great Enrichment" (2020) 37:5 *Asia Pacific Journal of Management*, online: <https://doi.org/10.1007/s10490-019-09648-2>.

Treiblmaier, Hermann. "Do Cryptocurrencies Really Have (No) Intrinsic Value?" (2022) 32 *Electron Markets* 1749–1758. Available online: <https://doi.org/10.1007/s12525-021-00491-2>.

U.S. Securities and Exchange Commission. Press Release. "Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay \$30 Million to Settle SEC Charges." 9 February 2023. Online. SEC. <www.sec.gov/news/press-release/2023-25>.

United States, Department of Justice, Southern District of New York. *Co-Founder of Multi-Billion-Dollar Cryptocurrency Pyramid Scheme "OneCoin" Pleads Guilty*. 16 December 2022. Online: <https://www.justice.gov/usao-sdny/pr/co-founder-multi-billion-dollar-cryptocurrency-pyramid-scheme-onecoin-pleads-guilty>.

United States, Department of Justice, Southern District of California. *Founder of Fraudulent Cryptocurrency Charged in \$2 Billion BitConnect Ponzi Scheme*. 25 February 2022. Online: <https://www.justice.gov/usao-sdca/pr/founder-fraudulent-cryptocurrency-charged-2-billion-bitconnect-ponzi-scheme>.

U.S. Commodity Futures Trading Commission, *An Introduction to Virtual Currency* (February 2018), online: CFTC https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/oceo_aivc0218.pdf.

United States Department of Justice, Office of Public Affairs. "Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving Over \$100 Million in Intended Losses." 30 June 2022. Online. Department of Justice. <www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud>.

Ushida, R., & Angel, J. (2021). "Regulatory considerations on centralized aspects of DeFi managed by DAOs." In M. Bernhard et al. (Eds.), *FC 2021* (pp. 21–36). LNCS, vol. 12676, Springer. https://doi.org/10.1007/978-3-662-63958-0_2

Vardi, Noah. 'Bit by Bit: Assessing the Legal Nature of Virtual Currencies.' In *Bitcoin and Mobile Payments: Constructing a European Union Framework*, edited by G. Gimigliano. London: Palgrave-Macmillan, 2016. 60-66.

Walch, Angela. "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems." In *Crypto Assets: Legal and Monetary Perspectives*, edited by Chris Brummer. Oxford: Oxford University Press, 2019. <https://doi.org/10.1093/oso/9780190077310.003.0003>.

Wright A, De Filippi P, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (March 10, 2015), online: SSRN <https://ssrn.com/abstract=2580664> or <http://dx.doi.org/10.2139/ssrn.2580664>

Wright A, De Filippi P, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (March 10, 2015), online: SSRN <https://ssrn.com/abstract=2580664> or <http://dx.doi.org/10.2139/ssrn.2580664>.

Yuyama, T., Katayama, K., Brigner, P. "Proposal of Principles of DeFi Disclosure and Regulation." In: Essex, A., et al. Financial Cryptography and Data Security. FC 2023 International Workshops. FC 2023. Lecture Notes in Computer Science, vol 13953. Springer, Cham, 2024. pp. 141–164. https://doi.org/10.1007/978-3-031-48806-1_10.

Zetsche, Dirk A. et al. "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators." 63 Harvard International Law Journal (forthcoming 2019).