DeFi: A Framework of the Automated Financial System

Vanessa Villanueva Collao*

Decentralized Finance, or DeFi, is the technological distribution of financial services empowered by blockchain. This alternative market deals with processes similar to traditional finance involving the creation, management, and investment of money and financial assets. However, the fundamental difference in DeFi gravitates around the multiple financial intermediaries substituted with applications that automatize cryptoassets trade (a kind of digital assets), among other financial activities. This Article explores the characteristics of DeFi and the relevant players.

I. INTRODUCTION 76
II. BLOCKCHAIN TECHNOLOGIES 78
A. *Consensus Protocols* 80
1. PoW 81
2. PoS 81
B. *Smart Contracts* 82
1. Execution and Formalization of Relationships 82
2. Limitations of Coded Law and Self-Execution 83
III. DEFI PART I: CRYPTOASSETS SALES AND SECURITIES REGULATION 84
A. *DAOs and Cryptoassets* 86
B. *The* Howey *Test, The Bahamas Test, and SAFTs* 87
IV. DEFI PART II: STRUCTURE AND MAJOR PLAYERS 91
A. *Major Players* 95
1. Coders 95
2. Decentralized Exchanges (DEXs) and Cryptoexchanges 97
3. Oracles 99
B. *Decentralized Lending (DeLe)* 100

---

* © 2024 Vanessa Villanueva Collao. Max Weber Fellow at the European University Institute. I would like to thank Vincenzo Zeno Zencovich, the South EU Data Governance Chair, and the University of Roma Tre for their support of this project, Robert M. Lawless for the insightful conversations on DeLe, the participants in the Corporate Governance Symposium at the University of Genoa for their helpful comments, and Berkeley Global Society. I appreciate the assistance of the University of Illinois Law Library. Usual disclaimers apply.

1. DeLe Protocols in DeFi 102
2. Flash Loans 104
3. Liquidations 105
C. *Derivatives* 106
1. DeFi Synthetic Assets 107
2. DeFi Derivatives 108
V. CONCLUSION 109

I. INTRODUCTION

It is 1988, and a group of techno-anarchists at the "Crypto '88" conference receive a short prompt, a *manifesto*, anticipating a world free from intellectual property barbed wires.[1] Per its author Timothy May, they imagined a place where interconnected computers would allow people to communicate anonymously, absent any external permission, and negotiate electronically without knowing their counterparties.[2] This world that Timothy May predicted is now known as blockchain.

Blockchain is a type of distributed ledger technology whose main features are decentralization and disintermediation.[3] Through the decentralization of processes, the cypherpunk community aimed to solve problems with centralized actors such as banks, which were deemed complicit in the financial crisis.[4] Indeed, decision-making in the blockchain ecosystem allegedly shifts from one actor to a distributed network of countless actors. The effect of decentralization is a lack of external control over systems deployed on the blockchain.[5] Therefore, reducing the number of required intermediaries is crucial to maintaining

---

1. Timothy May, *The Crypto Anarchist Manifesto*, ACTIVISM.NET, (Nov. 22, 1992), https://www.activism.net/cypherpunk/crypto-anarchy.htmlhttps://www.activism.net/cypherpunk/crypto-anarchy.html [https://perma.cc/9WC9-KJFQ].

2. Timothy May was the founder of the cryptoanarchist movement during the '90s that boosted cypherpunks' focus on certain types of technologies to promote privacy from the government and, thus, freedom. *Id.*

3. ARVIND NARAYANAN, JOSEPH BONNEAU, EDWARD FELTEN, ANDREW MILLER & STEVEN GOLDFEDER, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION 27, 278 (2016).

4. During the years following the 2008 financial crisis, a disgruntled community of coders (developers) actively helped, through a series of email exchanges, Satoshi Nakamoto, who claimed to be a thirty-six-year-old man, in creating a privately coined currency, Bitcoin. Joshua Davis, *The Crypto-Currency: Bitcoin and its Mysterious Inventor*, NEW YORKER (Oct. 3, 2011), https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

5. PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 6 (2018).

the system altogether. In blockchain, intermediaries are replaced by protocols and coded rules that operate in a quasi-deterministic way.[6]

The erosion of trust in financial intermediaries nurtured the cypherpunk philosophy behind blockchain to democratize access to capital and information. This Hayekian vision of trust has ignited interest in the function of money, the role of governments, and their privilege to coin money.[7] Following this trend, cypherpunks, supreme believers of individual choice, created a system hidden from governments where technology could code ideas into cash value.[8] While several attempts have been made over the years, only with Bitcoin has a private electronic monetary system become a reality.[9]

In the aftermath of the explosion of privately coined currencies (cryptocurrencies), the development of several technological infrastructures dissolved Cypherpunk's initial goals of privacy by overcoming government surveillance using technology. Today, May's crypto-anarchist vision has turned into a decentralized market where participants interact in a unique ecosystem that privileges faster (and safer) financial services and products. This Article centers on an ecosystem called Decentralized Finance, or DeFi.

It is still unsettled whether the boundaries of DeFi intersect with traditional financial systems. For some, the main distinction between Open Financial Systems and DeFi resides in infrastructure centralization. In Open Finance, traditional banking services integrate API systems and blockchain to improve transparency, accountability, and transaction rates

---

6. *Id.* at 134.

7. For the Nobel Laureate to avoid excessive control over a monetary system, government-issued currencies were to be substituted with private ones, which would allow people to make dealings in a currency they repose trust. FRIEDRICH A. HAYEK, CHOICE IN CURRENCY: A WAY TO STOP INFLATION 19 (The Inst. Of Econ. Affs., 1976). As with fiat money, many experiments in the world have created a medium of exchange without extrinsic value. Giant Yap stones have been traded for decades in exchange for goods and services. For these stones to function as a medium of exchange, they needed to represent purchasing power and be acknowledged by others. Thus, they needed to be trusted and serve as a "memory [or record] of contributions". Michael F. Bryan, *Island Money, Econ. Comment.* (Feb. 1, 2004), https://www.clevelandfed.org/publications/economic-commentary/2004/ec-20040201-island-money [https://perma.cc/83JT-SUFY].

8. Bradly Dale, *Cypherpunk, Crypto Anarchy and How Bitcoin Lost the Narrative*, COINDESK:TECH (Sept. 14, 2021, 12:34 AM), https://www.coindesk.com/tech/2020/11/24/cypherpunk-crypto-anarchy-and-how-bitcoin-lost-the-narrative [https://perma.cc/98S7-6ZK8].

9. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008), https://bitcoin.org/bitcoin.pdf. The history of Bitcoin is a history of failures that build up the current blockchain system. Among the more than forty projects to achieve peer-to-peer cash systems, PayPal (the one with a strong intermediation architecture) is still active. NARAYANAN ET AL., *supra* note 3, at ix.

without resorting to cryptomarkets.[10] On the contrary, DeFi uses blockchain infrastructure as its core business model, issuing or employing digital assets to create alternative financial products and experiences potentially without prior ownership. There are many phenomena that exist in traditional finance, such as dispersion of ownership when going public—namely, the regulated process of private companies resorting to the public to raise capital in exchange for stock (i.e., Initial Public Offerings or IPOs). Such phenomena are not observable in DeFi.

Finance and financial products have constantly been objects of regulatory oversight. However, blockchain has modified our conception of how businesses are developed, making it harder to fall under regulation. As a result, many areas of the law must be reconsidered or reframed.

This Article offers a glimpse into this automated financial system, debunks some common myths and assumptions around blockchain technology, and provides a holistic approach to exploring cryptomarkets from a legal perspective. Part II briefly introduces blockchain technologies and the role of smart contracts in DeFi. Part III offers an overview of cryptoassets' sales and securities regulation applications and challenges. Part IV identifies DeFi's structure, major players, and primary financial services. Finally, the Article concludes in Part V.

II. BLOCKCHAIN TECHNOLOGIES

More than a utopian vision of a parallel society, blockchain is the aggregation of a series of fields, ranging from cryptography to economics, developed over the years. Indeed, the process of disintermediation has a long history, initiated with the internet and now boosted by blockchain or Web 3.0.[11]

---

10. Application programming interface (API) is a type of software interface, a set of protocols and codes that enable communication and sharing of information among different platforms. *See What is an Application Programming Interface (API)?*, IBM, https://www.ibm.com/topics/api [https://perma.cc/J26X-GAZJ]. APIs offer data-sharing services to third parties, acting as an intermediary. *Open Finance vs. Decentralized Finance*, CRYPTOPEDIA (June 28, 2022), https://www.gemini.com/cryptopedia/open-vs-decentralized-finance-defi.

11. The web stages of this disintermediation, from being a consumer of static information to owning or providing value from content, are known as web 1.0, web 2.0, and web 3.0. Umesha Naik & D. Shivalingaiah, *Comparative Study of Web 1.0, Web 2.0 and Web 3.0*, INT'L CALIBER 499 (2008). For more on Web 3.0 infrastructure, see Katt Gu & Lorraine Zhou, *Web 3.0 Revolution: Infrastructure, Applications, and Opportunities* (2023) (unpublished manuscript) (on file with author).

Blockchain technology is not only a registry that functions as a memory of contributions.[12] Rather, it potentially records anything that can be digitized.[13] As part of one of the DLT technological infrastructures, blockchain is used to access, validate, record, update, and store information among computers (peers or nodes).[14] Blockchain makes records immutable by certifying them through hash functions.[15] Any record or information is linked to a unique number that changes with a minor change in the original document.[16]

Moreover, blockchain allows the collaborative development of autonomous software through multiple actors (peers or nodes) dispersed across various jurisdictions.[17] Consequently, once the software is completed, its deployment on a blockchain makes those systems autonomous. In theory, decentralization implies that once created, the system is not controlled by a single party.[18] Therefore, blockchain's transnational element reflects a disregard for specific legal constraints during the creation of those systems. Put differently, when developers (broadly speaking) define the coded rules, those rules are not the product of law but an agreement on instructions and incentives to support that system.[19]

In this way, the infrastructure built around blockchain enables the issuance of value through digital assets (cryptoassets) and the direct (disintermediated) transfer of value. Thus, because the constituents of the transaction are substituted with computer code, this architecture reduces the costs of transferring that value.[20] Likewise, blockchain has also

---

12. Bryan, *supra* note 7.

13. Recently, the whole genomic sequence of the DNA has been encrypted and stored in blockchain, guaranteeing pseudonymity by masking the identities using technologies such as zero-knowledge-proofs. Dennis Grishin, Kamal Obbad & George M. Church, *Data Privacy in the Age of Personal Genomics*, 37 NATURE BIOTECH. 1115, 1115-16 (2019).

14. CAROL GOFORTH & YULIYA GUSEVA, REGULATION OF CRYPTOASSETS 774 (2d ed. 2022).

15. Stuart Haber & W. Scott Stornetta, *How To Time-Stamp a Digital Document*, 3 J. CRYPTOLOGY 99, 109-10 (1991).

16. Before blockchain/DLT technologies, a public ledger used for the registration and display of hash was *the New York Times*. Daniel Oberhaus, *The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995*, VICE: MOTHERBOARD (Aug. 27, 2018, 3:19 PM), https://www.vice.com/en/article/j5nzx4/what-was-the-first-blockchain [https://perma.cc/KE9R-EMWE].

17. NAKAMOTO, *supra* note 9, at 8.

18. NARAYANAN ET AL., *supra* note 3, at 66.

19. De Filippi & Wright, supra note 5, at 44-45.

20. Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 534 (2018).

managed to reduce coordination costs in order to detect (not prevent) the attacks on the protocol, solving the double spending problem of electronic transactions through consensus mechanisms.[21]

A. *Consensus Protocols*

Blockchain uses gaming reward mechanisms to verify information entries. These mechanisms are labeled consensus protocols. The goal of consensus is to solve the double spending attack—stop redeeming a transaction input twice. This means limiting the use of digital assets by detecting when a *coin* has already been used. For this purpose, the coin must contain some personal information that only the true user can decode. Before blockchain, the double spending issue was central to online payments. There was no effective way to detect fraudulent offline use without a trusted centralized authority that publishes the transactions, albeit not in real-time.[22]

The Nakamoto consensus of Bitcoin solves this problem, allowing network participants to concur on transaction validity and, eventually, on its registration in an immutable public ledger.[23] In other words, transaction processing happens when the majority of the nodes agree on the transactions' legitimacy and validity before recording them.[24] Thus, consensus acts as a voting mechanism.

The concept of consensus is tied to the *Sybil* resistance mechanisms.[25] In an ecosystem that is allegedly trustless and permissionless, the threat of malicious attacks is latent. A node can reach the network with multiple identities used to gain power and influence in the agreement of the transactions. For this reason, detecting Sybil attacks in a decentralized system requires proof of a specific resource (the unique identity), which is almost impossible to forge.[26] Currently, there are two

---

21. NARAYANAN ET AL., *supra* note 3, at 22.

22. Blockchain consensus mechanisms expand the several attempts to overcome the double spending problem. Specifically, cypherpunks implemented the patented blind signature of DigiCash (where only one of the parties identities is tied to the coin and is the sole one to decode it). However, DigiCash failed because there was no peer-to-peer option, and centralized authorities were required. David Chaum, *Achieving Electronic Privacy*, 267 SCI. AM. 96, 98 (1992).

23. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll & Edward W. Felter, *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, IEEE SYMP. ON SEC. AND PRIV. 104, 105 (2015).

24. *Id.* at 107.

25. *Id.*

26. For a block transaction to be valid, it needs at least fifty-one percent of the nodes to agree on the current state of the network. Preethi Kasreddy (@iam_preethi), *People Confuse[s]*

major crypto Sybil mechanisms: proof-of-work (PoW) and proof-of-stake (PoS).

1. PoW

In PoW, the nodes agree on solving a complicated puzzle as the key to settling the transfer of property without needing a clearinghouse or intermediary.[27] The peculiarity of PoW is that the consensus and Sybil resistance mechanisms conflate.

The incentives on PoW work are simple: the first member announces the solution of a mathematical puzzle and showcases it to other members, who in turn will run a quick check and decide to allocate the block—a block reward, crediting the member some amount of Bitcoin along with transaction fees.[28] While the technology eradicates intermediaries, the consensus algorithm restores trust among parties that do not know each other and helps them to engage in transactions. This incentive mechanism makes it almost impossible to revert a transaction unilaterally since it would be excessively expensive for the majority of nodes to coordinate and decide on an attack.

2. PoS

The criticalities of computer power and energy consumption have encouraged alternative Sybil resistance processes. The relevance of PoS resides in the selection of specific validators of the transactions according to the number of cryptoassets they hold rather than solving a mathematical puzzle.[29]

PoS has gained some attention since the major blockchain, Ethereum, changed its proof of resources from PoW to PoS.[30] Most DeFi transactions use the Ethereum blockchain to include other forms of information, such as software or computer programs called smart contracts.

Consensus Algorithms vs. Sybil Resistance Mechanisms, X (Jan. 20, 2022, 11:09 AM), https://x.com/iam_preethi/status/1484211555281559554?lang=en [https://perma.cc/U244-SFD2].

27. Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain*, 63 COMMS. ACM 80, 83 (2020).

28. NAKAMOTO, *supra* note 9, at 4.

29. Fahad Saleh, *Blockchain Without Waste: Proof-of-Stake*, 34 REV. FIN. STUDS. 1156, 1157 (2020).

30. *The Merge*, ETHEREUM FOUND., https://ethereum.org/en/upgrades/merge [https://perma.cc/33DT-S6JT] (last updated Apr. 24, 2024).

B. Smart Contracts[31]

Smart contracts are computer programs that memorialize messages with computer code. They run on the Ethereum blockchain using programming languages such as Solidity. When the active peers agree, the transaction is completed and becomes immutable. Smart contracts use the logic of "if this, then that" to issue and transfer cryptoassets, record information, and implement or grow governance systems.[32]

A smart contract operates with two accounts: a personal (externally owned) account and a contract account. The interaction between two personal accounts results in the transfer of cryptoassets (frequently ether). The interaction between a personal account and a contract account triggers a smart contract (which, in turn, can contain or trigger another contract account). The interaction between two smart contract accounts is fundamental for DeFi since they build up what is called intra-transaction composability, a way to keep up promises and settle transactions.[33] Before the execution, a small fee (called gas) is assessed for every step.[34]

1. Execution and Formalization of Relationships

Smart contracts are essential for DeFi because they capture the understanding of commercial transactions with computer code directly or indirectly, giving execution to all or to certain provisions of an agreement.[35] However, there are caveats to consider when comparing smart contracts with legal contracts.[36]

---

31. Gu & Zhou, *supra* note 11.

32. *Ethereum Whitepaper*, ETHEREUM FOUNDATION, https://ethereum.org/en/whitepaper [https://perma.cc/P7BD-JZ3M] (last updated Mar. 13, 2024).

33. Fabian Schär, *DeFi's Promise and Pitfalls*, INT'L MONETARY FUND: FIN. & DEV., Sept. 2022, at 33, 34. https://www.imf.org/en/Publications/fandd/issues/2022/09/Defi-promise-and-pitfalls-Fabian-Schar [https://perma.cc/EN7H-JTGV]. For further analysis of demystification in DeFi, see Part II.

34. DE FILIPPI & WRIGHT, *supra* note 5, at 29.

35. Stuart D. Levi & Alex Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ [https://perma.cc/8DW4-82RB].

36. The literature on smart contracts has illustrated that smart contracts often fall short of fulfilling or replacing traditional contracts. See André Udo Janssen & Francesco Paolo Patti, *Demistificare Gli Smart Contracts [Smart Contracts' Demystification]*, 1 OSSERVATORIO DEL DIRITTO CIVILE & COMMERCIALE [OBSERVATORY OF CIV. & COM. L.] 31, 46 (2020) (indicating which types of contracts are difficult to implement in smart contract code); Andres Guadamuz, *All Watched Over by Machines of Loving Grace: A Critical Look at Smart Contracts*, 35 COMPUT. L. SEC. REV. 105338 (2019) (explaining how the technicalities of the smart contract drive the inclusion of smart contracts into legal categories); Primavera De Filippi, Chris Way & Giovanni

The recurrent example is one of the vending machines.[37] Although, from a close look, the actions that can be performed with a vending machine are different. In an exchange with a vending machine, only one of the party's obligations is automated, while the other requires some external human input. Contrarily, in a smart contract, both parties' actions are automated, and no future obligations remain to be executed.[38]

Since the obligations of both parties are automated, the synchronous feature of a smart contract emerges, allegedly transforming lines of code into a self-enforcing and self-executing contract.[39] This description of the characteristics of smart contracts is much more in line with contracts of adhesion (U.S. click-wrap contracts). Following that description, there is no place for bargaining or negotiation and a lack of human connection. Only *ex-ante* formalizations appear because computers do not exchange promises; thus, there is little room for *ex-post* decision-making.[40]

2. Limitations of Coded Law and Self-Execution

Generally speaking, smart contracts raise no issues when the contract is perfected elsewhere, and the instructions of all or some parts of the agreement are then deployed in a smart contract (natural contract laws will regulate the transaction). Conversely, issues arise when there is no preliminary agreement or when the set of instructions is memorialized and compiled in bytecode (directly written on a smart contract code) and deployed.[41] Thus, in that case, there would be no space for contractual interpretation or reverting the transaction to an *ex-ante* status quo with the sole resort to restitutionary measures.[42]

Indeed, the nucleus of smart contracts is that the operational semantics of the coded rules do not mirror the denotational semantics,

---

Sileno, *Smart Contracts*, 10 INTERNET POL'Y REV. (Special Issue) 1, 5 (2021) (indicating a series of misconceptions regarding the operativity, nature, and scope).

37. Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 315 (2017) (comparing extensively smart contracts with vending machines).

38. Farshad Ghodoosi, *Contracting in the Age of Smart Contracts*, 96 WASH. L. REV. 51, 64 (2021).

39. Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 319-20 (2017).

40. Ghodoosi, *supra* note 38, at 79; *see also* Alberto Maria Gambino & Andrea Stazi, *Contract Automation from Telematic Agreements to Smart Contracts*, 7 ITALIAN L.J. 97, 109-10 (2021).

41. DE FILIPPI & WRIGHT, *supra* note 5, at 5.

42. Ghodoosi, *supra* note 38. However, the jurisdiction assessment could be challenging.

namely their intended meaning.[43] These coded rules are developed without consideration of business practices or regulations.[44]

The deterministic nature of smart contracts does not account for the great majority of business contracts or relational contracts, where the contract formation occurs over time instead of a specific time for the "meeting of the minds."[45] However, the development of complex smart contracts follows several implementations to the execution part through multi-signature wallets and verification. In this sense, many smart contracts' ultimate execution can be halted until a complete agreement on the performance is reached.[46]

In the event of breach, a designated arbitrator can determine the outcome in several ways, through specific provisions included in the smart contract, by utilizing blockchain adjudication systems, or via online dispute resolution systems.[47] Admittedly, not all smart contracts are spot contracts with an immediate effect or execution. The blockchain community is well aware of that and has taken it into account for the development of DeFi ecosystems that offer lending products with embedded remedies similar to repo mechanisms, such as flash loans.[48]

III. DEFI PART I: CRYPTOASSETS SALES AND SECURITIES REGULATION

Cryptoassets' nature has attracted numerous scholars to decipher their scope and to outline the boundaries of blockchain technology and

---

43. Tom Butler, Firas Al Khalil, Marcello Cecil & Leona O'Brien, *Smart Contracts and Distributed Ledger Technologies in Financial Services: Keeping Lawyers in the Loop*, 36 BANK & FIN. SERV. POL'Y REP. 1, 6 (2017).

44. Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law*, 82 MOD. L. REV. 207, 207-8 (2019).

45. These types of contracts or contractual relationships are crucial for business operations and strategy, especially when they involve actions that cannot be specified in advance, making formal contracts unsuitable. These informal relationships are built over time and encourage collaboration among the parties. *See generally* Stewart Macaulay, *Non-Contractual Relations in Business: A Preliminary Study*, 28 AM. SOCIO. REV. 55 (1963). *See also* Ian R. Macneil, *Contracts: Adjustment of Long-Term Economic Relations under Classical, Neoclassical, and Relational Contract Law*, 72 NW. U. L. REV. 854 (1978) (discussing flexible patterns for the production and distribution of goods and services).

46. Werbach & Cornell, *supra* note 39, at 322.

47. *Id.* at 347. *See also* Pietro Ortolani, *Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin*, 36 OXF. J. LEG. STUD. 595, 611 (2016) (explaining models of online dispute resolution using blockchain technology); Florian Möslein, *Legal Boundaries of Blockchain Technologies: Smart Contracts as Self-Help?*, *in* DIGITAL REVOLUTION—NEW CHALLENGES FOR LAW 313 (Alberto De Franceschi & Reiner Schulze eds., 2019) (describing self-help remedies and blockchain-based adjudication systems).

48. *See discussion infra*, Part III.

their expansion into the regulated financial world. Cryptoassets are a type of digital asset, sometimes of hybrid nature, that perform different tasks in blockchain.[49] Indeed, cryptoassets are a heterogeneous group of digital assets, but the term cryptocurrencies has been commonly used in their substitution. Although cryptocurrencies, as the name implies, possess a monetary function, the uses of cryptoassets are manifold and do not necessarily perform such a monetary function. Cryptoassets are used to monitor supply chains,[50] data sharing, digital voting, record real estate, insurance,[51] record/certify intellectual property,[52] and weapon tracking, among others.[53]

In DeFi, cryptoassets facilitate payment processing, clearing and settling financial transactions, and equity trading.[54] There are several advantages of cryptoassets, although they have gained great attention because of their employment as a financial instrument and their prominent role in raising capital to fund projects following the rise of decentralized autonomous organizations.[55]

---

49. Yuliya Guseva, *A Conceptual Framework for Digital-Asset Securities: Tokens and Coins as Debt and Equity*, 80 MD. L. REV. 166 (2021). *See also* Parma Bains, Arif Ismail, Fabiana Melo & Nobuyasu Sugimoto, *Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets*, INT'L MONETARY FUND: FINTECH NOTE, Sept. 2022, at 4.

50. Vishal Gaur & Abhinav Gaiha, *Building a Transparent Supply Chain*, HARV. BUS. REV., May-June 2020, at 2. Blockchain impacts the supply chain not only in terms of efficiency by reducing processes but also in terms of sustainability, shortening the path to paperless solutions. Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis & Lejia Shen, *Blockchain Technology and Its Relationships to Sustainable Supply Chain Management*, 57 INT. J. PROD. RES. 2117, 2122 (2019).

51. The convergence of insurance and blockchain has opened the door for a wide range of conventional and emergent applications, such as insurance in travel, life, accident, claims management, securities, digital identities, smart contracts, and reinsurance (the insurance of the insurer). Ankitha Shetty, Adithya D. Shetty, Rashmi Yogesh Pai, Rohini R. Rao, Rakshith Bhandary & Jyothi Shetty, *Block Chain Application in Insurance Services: A Systematic Review of the Evidence*, 12 SAGE OPEN, Jan.-Mar. 2022, at 8. *See also* D. Popovic, C. Avis, M. Byrne, C. Cheung, M. Donovan, Y. Flynn, C. Fothergill, Z. Hosseinzadeh, Z. Lim & J. Shah, *Understanding Blockchain for Insurance Use Cases*, 25 BR. ACTUAR. J. 1, 8 (2020).

52. *See* IGNACIO DE LEON, MONETIZATION OF TRADE SECRETS UNDER BLOCKCHAIN: THE NEXT STEP IN INTELLECTUAL PROPERTY COMMERCIALIZATION (unpublished manuscript) (on file with author).

53. GOFORTH & GUSEVA, *supra* note 14, at 13.

54. Raphael Auer et al., *The Technology of Decentralized Finance (DeFi)* (Bank for Int'l Settlements, Working Paper No. 1066, 2023).

55. *See* DAVID MEIRICH, DECENTRALIZED AUTONOMOUS ORGANIZATIONS (unpublished manuscript) (on file with author); Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, 4.2 STAN. J. BLOCKCHAIN L. POL'Y 152, 157 (2021).

A. *DAOs and Cryptoassets*

Decentralized autonomous organizations (DAOs) are cryptoasset-based ventures that rely on blockchain and smart contract code as a source for governance by defining and encoding some or all of their rules.[56] Towards the end of the 2010s, DAOs became incredibly popular as numerous projects were developed in permissionless blockchains. Promoters financed these ventures using low-funding mechanisms that override securities regulations. These mechanisms are labeled Initial Coin Offerings (ICOs).[57]

The name choice is not a coincidence. An ICO purports to mirror an IPO, a regulated and expensive process to raise capital by selling shares to the public. However, the number of intermediaries that assist a company during an IPO (broker-dealers, underwriters, lawyers, auditors, etc.) is substituted with a platform mechanism where investors exchange fiat currency (usually U.S. dollars) for cryptoassets. Most of the time, this process involves a cryptoassets pre-sale,[58] a hard-cap or soft-cap (the maximum or minimum amount requested for funding), code disclosures,[59] a white paper, KYC procedures,[60] and frequently a crypto exchange.[61]

The ICO trend continued undisturbed until 2017 when the SEC released the DAO Report, sending a strong message to the entire

---

56. DE FILIPPI & WRIGHT, *supra* note 5, at 137. Most of the enterprises approaching blockchain technology start with Decentralized Organizations (DOs) and progressively become autonomous systems. *Id.* at 148. Nowadays, the term DAOs encompasses both organizations.

57. Laura Shin, *Here's the Man Who Created ICOs and This Is the New Token He's Baking*, FORBES (Sept. 21, 2017, 12:06 PM), https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/?sh=117200291183; JAY B. SYKES, CONG. RSCH. SERV., R45301, SECURITIES REGULATION AND INITIAL COIN OFFERINGS: A LEGAL PRIMER 1 (2018).

58. Saman Adhami, Giancarlo Giudici & Stefano Martinazzi, *Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings*, 100 J. ECON. BUS. 64, 67 (2018).

59. Giancarlo Giudici & Saman Adhami, *The Impact of Governance Signals on ICO Fundraising Success*, 46 J. IND. BUS. ECON. 283, 300 (2019). Code disclosures are strongly connected to the development of the code on GitHub. Sabrina T. Howell, Marina Biessner & David Yermack, *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales*, 33 REV. FIN. STUD. 3925, 3941 (2020).

60. There is little information on whether these procedures are consistent with KYC in IPOs. Vanessa Villanueva Collao, *Empirical Methods in Comparative Law: Data Talks*, 12/2 COMP. L. REV. 55, 78 (2023).

61. Paul P. Momtaz, *Initial Coin Offerings*, 15 PLOS ONE 1, 3 (2020). These empirical analyses reflect legal scholarship on the main elements connected to disclosures. Chris Brummer, Trevor I. Kiviat & Jai Massari, *What Should Be Disclosed in an Initial Coin Offering?*, *in* CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 157 (Chris Brummer ed., 2019).

cryptocommunity (with a particular focus on investors) about the perils of these unregulated mechanisms.[62] The report explained that the German corporation Slock.it initiated the process of issuing cryptoassets (called DAO tokens) through one of the largest cryptoasset sales (ICOs), the Genesis DAO (The DAO). The DAO's purpose was to create a platform that would fund other blockchain projects. DAO tokens were allegedly imbued with some governance rights allowing companies to propose projects and obtain funding if voted.[63] The DAO is the startling point of the SEC regulation by enforcement of technological developments that collide with securities regulations. Specifically, the DAO was the first tentative in the U.S. to explore the question of whether cryptoassets were securities.[64]

B. The Howey Test, The Bahamas Test, and SAFTs

The nature of cryptoassets as a security is not yet settled. Several scholars have devoted efforts to bringing back a cryptoasset taxonomy. Some classify cryptoassets within the category of commodities and others as securities, further distinguishingthem as equity or bonds.[65] This distinction is evidenced by the different stages of cryptoassets' hybrid nature.[66] Before the ICO, these projects lack any ownership structure. During the ICO and right after the sale, cryptoassets behave like bonds, and when the projects are developed and launched cryptoassets resemble equity.

The U.S. Securities Act provides a definition of securities, their registration and disclosure requirements, while Section 10(b) of the Exchange Act regulates fraudulent conduct involving securities.[67] This definition of securities is expanded through the catch-all provision of

---

62. Press Release, SEC, *SEC Releases Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities* (July 25, 2017), https://www.sec.gov/news/press-release/2017-131 [https://perma.cc/N5SJ-4BXS] [hereinafter Press Release, SEC, *Investigative Report Concluding DAO Tokens were Securities*].

63. GOFORTH & GUSEVA, *supra* note 14, at 248.

64. Press Release, SEC, *Investigative Report Concluding DAO Tokens were Securities*, *supra* note 62.

65. For an analysis exploring cryptoassets in the form of equity, see Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, 60 HARV. INT. L.J. 267 (2019). For an analysis of cryptoassets as debt, see Guseva, *supra* note 49, at 184.

66. Carol R. Goforth, *Crypto is Money, Property, A Commodity, and a Security, All at the Same Time*, J. FIN. TRANSFORM. 102 (2019).

67. The Securities Act, 15 U.S.C. § 77b(a)(1); Securities and Exchange Act, 15 U.S.C. § 78j(b).

investment contracts, where the nature of securities is assessed on a case-by-case court analysis, following the principle of substance over form.[68] Nevertheless, it appears that securities regulation is too old to accommodate the multiple issues arising from cryptoasset sales.

An investment contract is assessed under a tri-partite test—the *Howey* Test—copiously glossed and interpreted by case law as an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial efforts of the promoter or others.[69] Nevertheless, when it comes to the decentralized nature of cryptoassets and the blockchain features, the third prong—the expectation of profits—is challenging to assess. As a result, academic proposals have partially implemented the *Howey* Test, adding a different one—the *Bahamas* Test—which emphasizes decentralization.[70] According to the *Bahamas* Test, the classification of a cryptoasset as a security depends on the project's ability to operate independently of the seller's external efforts.[71] The Securities and Exchange Commission (SEC) applied this test successfully, but it has not been of guidance for cryptoassets issuance.[72] The SEC's enforcement actions seemed erratic at times, which led to instances where neither test was applied, but the outcome of cryptoassets being classified as securities was ensured.[73]

With law enforcement's gatekeeping role in assessing cryptoassets as securities, even private agreements coming from the industry have not faced a different outcome. The Safe Agreement for Future Tokens (SAFT) was modeled along the same lines as the Safe Agreement for

---

68. Both Acts define an investment contract as a security in Section 3(a)(10) of the Exchange Act and Section 2(a)(1) of the Securities Act. *See* 15 U.S.C. § 78c(a)(10); 15 U.S.C. § 77b(a)(1). However, the interpretation and contextualization of both definitions are analyzed in light of the *Howey* Test. SEC v. W. J. Howey Co., 328 U.S. 293 (1946).

69. An investment contract is "a contract, transaction, or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or third party." *Howey*, 328 U.S. at 298-99; *see also* SEC v. Edwards, 540 U.S. 389, 393 (2004).

70. M. Todd Henderson & Max Raskin, *A Regulatory Classification of Digital Assets: Toward an Operational* Howey *Test for Cryptocurrencies, ICOs, and Other Digital Assets*, COLUM. BUS. L. REV. 443, 461 (2019).

71. *Id.* The first prong follows the Substantial Steps Test, which inquires about the promoter's good faith in developing a product (connected to a cryptoasset) that has some utility beyond the expectation of profits to be excluded from the realm of investment contracts.

72. United States SEC v. Kik Interactive Inc., 492 F. Supp. 3d 169, 177 (S.D.N.Y. 2020).

73. Carol R. Goforth, *Cinderella's Slipper: A Better Approach to Regulating Cryptoassets as Securities*, 17 HASTINGS BUS. L.J. 271, 282 (2021).

Future Equity (SAFE) to finance early-stage companies.[74] SAFT was developed to create a shielded/safe environment for valuable projects, creating functional cryptoassets (utility tokens) and avoiding chilling innovation. The proposal considered the two stages of pre-sale and sale (creation/distribution). Nevertheless, SAFTs did not guarantee securities regulation compliance or eliminate the risks of regulatory enforcement.[75] Indeed, the SEC's substance-over-form approach had not spared SAFTs, eventually leaving projects facing securities liability charges.[76]

When it comes to cryptoasset sales, there is a missed functional analysis of both ICO and IPO schemes, thereby considering an ICO as a virtual continuation of an IPO (with similar crowdfunding characteristics).[77] The periodic disclosure requirements were established for IPOs following the 1929 crash, intending to regulate companies that went public right after the New Deal. However, internet development has quickly demonstrated the inefficiencies of the disclosure system.[78]

For retail or unsophisticated investors, the quality of the information released is detrimental/insufficient to make informed choices.[79] There are two recurrent releases during an ICO: the white paper and code disclosure. While the white paper attracts more retail investors due to the

---

74. Juan Batiz-Benet, Jesse Clayburgh & Marco Santori, *The SAFT Project: Toward a Compliant Token Sale Framework*, SAFT PROJECT (Oct. 2, 2017), https://saftproject.com/ [https://perma.cc/SRB2-HPP4]; GOFORTH & GUSEVA, *supra* note 14, at 286.

75. Wright et al., *Not So Fast—Risks Related to the Use of a "SAFT" for Token Sales*, CARDOZO BLOCKCHAIN PROJECT 3 (2017), https://larc.cardozo.yu.edu/blockchain-project-reports/1/ [https://perma.cc/B3WN-HPWW].

76. The SEC has targeted high-profile issuers. *See, e.g., Kik Interactive*, 492 F. Supp. 3d at 173; Complaint at 3, SEC v. Telegram Group Inc., 448 F. Supp. 3d 352 (S.D.N.Y. 2020) (No. 1:19-cv-09439-PKC). Telegram Group eventually settled. *See* Press Release, SEC, *Telegram to Return $1.2. Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges* (June 26, 2020), https://www.sec.gov/news/press-release/2020-146 [https://perma.cc/2L8Y-ZH9T].

SAFTs also pose issues with agencies contending overlapping enforcement, exemplified in the case of Ripple between the SEC and the FinCEN (a bureau of the Department of Treasury for Financial Crimes Enforcement). GOFORTH & GUSEVA, *supra* note 14, at 327.

77. Alexis Collomb, Primavera De Filippi & Klara Sok, *Blockchain Technology and Financial Regulation: A Risk-Based Approach to the Regulation of ICOs*, 10 EUR. J. RISK REG. 263 (2019).

78. As happened with the IPOs' valuations during the late '90s dotcom bubble. *Id.* at 297.

79. Resulted in more than eighty percent of cryptoasset scams in 2017. GUSEVA & GOFORTH, *supra* note 14, at 290 (citing Ana Alexandre, *New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams*, COINTELEGRAPH (July 13, 2018), https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams [https://perma.cc/AC9R-L9GB]). The vast majority of cryptoinvestors do not possess the skills to ferret out scams, even when devoting time to "understanding" the projects. Paul P. Momtaz, *Is Decentralized Finance (Defi) Efficient?* (2022) (unpublished manuscript), https://ssrn.com/abstract=4095397 [https://perma.cc/UT7E-GTWW].

high returns statements, the code has crucial information about the entire project, particularly promoters' vested positions, options, and lock-up provisions.[80] Most of these provisions allow for a continuation of ownership and control.[81] However, code disclosures are rarely subject to a level of auditing that translates and verifies the same information (especially the promises) in natural language through the white paper or that can confer reliability to the project through risk factors.[82] Furthermore, the pseudonymous nature of blockchain increases instances of fraud.

All those challenges have not stopped the SEC's leading role in worldwide enforcement.[83] The SEC's regulation by enforcement had a countereffect on cryptoasset sales (ICOs), constraining many projects to resort to venture capital.[84] This shift constitutes an information loss and a regulatory limitation imposed on new projects absent proper guidance.[85] The lack of adequate cryptoasset transactions regulation resides in the belief that regulation creates a chilling effect on innovation and determines a migration to other jurisdictions. Nevertheless, there is no empirical evidence that more regulation in this area increases a change in the jurisdiction of blockchain projects.[86]

There are current initiatives, such as the Biden Executive Order for a framework on cryptoassets and a bipartisan proposal for cryptoasset

---

80. *Digital Asset and "Crypto" Investment Scams—Investor Alert*, SEC (Sept. 1, 2021), https://www.sec.gov/oiea/investor-alerts-and-bulletins/digital-asset-and-crypto-investment-scams-investor-alert [https://perma.cc/3W8H-HLFR]. These sales often employ fake testimonials to guarantee high returns. *See, e.g.*, Press Release, SEC, *SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security* (Oct. 3, 2022), https://www.sec.gov/news/press-release/2022-183 [https://perma.cc/MJ8L-KE3Q]. For an empirical analysis of ICO promises and lock-up provisions, see Shaanan Cohney, David Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591, 614 (2019).

81. Brummer et al., *supra* note 61, at 163.

82. Vanessa Villanueva Collao & Verity Winship, *The New ICO Intermediaries*, 5 ITALIAN L.J. 731, 749-50 (2019); Brummer et al., *supra* note 61, at 177.

83. Yuliya Guseva, *When the Means Undermine the End: The Leviathan of Securities Law and Enforcement in Digital-Asset Markets*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 1, 60 (2022); Douglas S. Eakeley & Yuliya Guseva, *Crypto-Enforcement Around the World*, 94 S. CAL. L. REV. PS. 99 (2021).

84. Guseva, *supra* note 83, at 30.

85. Verity Winship, *Private Company Fraud*, 54 U.C. DAVIS L. REV. 663, 709 (2020). Companies going private results in lesser amounts of corporate information facilitating securities fraud due to the lack of scrutiny and enforcement. Elizabeth Pollman, *Private Company Lies*, 109 GEO. L.J. 353, 377 (2020).

86. Brian D. Feinstein & Kevin Werbach, *The Impact of Cryptocurrency Regulation on Trading Markets*, 7 J. FIN. REGUL. 48, 82-88 (2021).

regulation in the U.S., that have different motivations.[87] The first one involves the threat of stablecoins to the current U.S. monetary/financial system, while the second aims for clarity in the realm of cryptoassets, guaranteeing certainty in enforcement. In contrast, the European MiCA and DLT regulation, as a more comprehensive approach to cryptomarkets, can help exploit the benefits of Web 3.[88] As this ecosystem moves at a swift pace, it seems an arduous task for regulators who continue chasing the technology. Cryptoassets are not the final step but the initial step on a series of products offered in blockchain and constitute the decentralized financial system.

IV. DEFI PART II: STRUCTURE AND MAJOR PLAYERS

The goal of disintermediation and decentralization in blockchain is to solve the problem of trust. DeFi creates an interactive ecosystem of transnational participants where smart contracts and open-source software/protocols allow for a technological distribution of financial services.[89] Decentralization is not a legal concept but refers to the factual state of the ecosystem. There is no current agreement on DeFi characteristics. Still, the main attributes are a transaction settlement on a permissionless blockchain, a direct transfer of value, and encoded rules in an open architecture.[90]

Scholars differ in views and exclude financial services from DeFi depending on the level of centralization and decentralization. However, decentralization is not constantly observed in blockchain. As this system develops, it forms a stack of layers that determines the level of centralization or decentralization needed. Indeed, it is likely to observe pieces of decentralization and centralization throughout blockchain. Specifically, in DeFi, decentralized pieces are re-centralized elsewhere.

---

87. Exec. Order No. 14,067, 87 Fed. Reg. 14,143 (Mar. 9, 2022); Lummis-Gillibrand Responsible Financial Innovation Act, S. 4356, 117th Cong. (2022).

88. The fears of systemic risk motivated the MiCA proposal. *Commission Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and Amending Directive (EU) 2019/1937*, at 1, COM (2020) 593 final (Sept. 24, 2020). In comparison, the need to create a sandbox for projects motivated the DLT proposal. Dirk A. Zetzsche, Filippo Annunziata, Douglas W. Arner & Ross P. Buckley, *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy*, 16 CAP. MARK. L.J. 203, 205 (2021).

89. Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, *Decentralized Finance*, 6 J. FIN REG. 172, 181-98 (2020).

90. David Gogel, *DeFi Beyond the Hype: The Emerging World of Decentralized Finance*, WHARTON BLOCKCHAIN & DIGIT. ASSET PROJECT (2021), https://wifpr.wharton.upenn.edu/research/ [https://perma.cc/ZRX6-XNAP].

Blockchain is composed of a stack of layers that builds the architectural foundations, such as L1/layer one (the settlement layer).[91] However, the immutability and rigidity of the blockchain architectural foundations inadvertently limited access to capital.[92] The transactional throughput (or scalability issues) showed the hardship of upgrading the system, precisely transforming a simple transfer of information every ten minutes to high-speed processing of a great number of transactions.[93] These issues determined the development of L2/layer two (the asset layer), creating cryptoassets on top of layer one.[94]

The specific contours of the DeFi infrastructure are construed on what computer scientists know as the application layer in blockchain.[95] However, these applications built on top of a blockchain infrastructure are subdivided into three types: (1) the protocol layer (L3/layer three), which are standards for on-chain management with a high level of interoperability; (2) the application layer (L4/layer four) connecting layer three protocols for the creation of decentralized applications (indeed, these applications provide a specialized software solution, which is commonly a service); and (3) the aggregation layer (L5/layer five) allowing users to benefit from the services offered by aggregating crucial information.[96]

---

91. Layer 1 (L1) comprises the technological foundations of blockchain, consensus algorithm, protocols, gaming reward incentives, block time, and, eventually, a dispute resolution system. *A Beginner's Guide to Understanding the Layers of Blockchain Technology*, COINTELEGRAPH, https://cointelegraph.com/learn/a-beginners-guide-to-understanding-the-layers-of-blockchain-technology [https://perma.cc/4Q2T-L5MZ] (last updated May 16, 2024).

92. Layer two (L2) is built on top of L1, improving transactions speed while maintaining decentralization. ABDELATIF HAFID, ABDELHAKIM SENHAJI HAFID & MUSTAPHA SAMIH, SCALING BLOCKCHAINS: A COMPREHENSIVE SURVEY, 8 IEEE ACCESS 125244, 125255 (2020). *See also* CLAUDE HUMBEL & FABRICE ECKERT, DECENTRALIZED EXCHANGES: FOUNDATIONS, RISKS, AND POLICY ISSUES, 1-20 (2023)(unpublished manuscript) (on file with author).

93. Having the three qualities of blockchain—decentralization, security, scalability—is impossible. Thus, one of them, scalability (or optimization of projects), must be sacrificed. Vitalik Buterin, *Why Sharding is Great: Demystifying the Technical Properties*, HACKERNOON (Apr. 7, 2021), https://hackernoon.com/demystifying-the-technical-properties-of-sharding-can-tell-us-why-it-is-great [https://perma.cc/YB2H-7RL4].

94. Fabian Schär, *Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets*, FED. RES. BANK ST. LOUIS REV. 153, 157 (2021).

95. Blockchain layered structure comprehends the hardware or infrastructure layer, the data layer (commonly the hash functions), the network layer (such as the peer-to-peer network of Bitcoin), the consensus layer (comprised of proof of resources and sybil resistant mechanisms), and the application layer (smart contracts and decentralized applications or dApps). COINTELEGRAPH, *supra* note 91.

96. Schär, *supra* note 94, at 156.

Most financial services and projects on blockchain are self-declared as DeFi projects, even if they possess a heavily centralized structure.[97] Therefore, it is unsurprising that this sub-field of blockchain supports most traditional finance products, with the main difference centered around the technological means employed. Traditional finance is often labeled CeFi (centralized finance),[98] yet traditional finance does not commonly implement its structure using blockchain technology. For this reason, when it comes to financial assets, a sound approach to distinguish traditional finance from financial ventures in blockchain is to divide them between:

- Traditional finance (no use of blockchain technology),
- CeFi (centralized protocols and cryptoassets representing financial products using blockchain technology), and
- DeFi (total decentralization of protocols and user control over cryptoassets).

Traditional finance has grown over decades, and governments have created a massive regulatory apparatus to create, manage, and invest money.[99] Contrarily, the disruption of blockchain technology developed a series of financial products that fall under the umbrella term DeFi without implying regulatory compliance and frequently being in the shadow of the financial system.[100]

Nevertheless, most current projects developed on DeFi are hybrid, using a decentralized/centralized system (a mix of CeFi and DeFi). In projects using a hybrid system, cryptoassets are non-custodial, which means that the user controls those financial assets.[101] Thus, no financial intermediaries hold these assets on the user's behalf. Moreover, within this spectrum, CeFi and DeFi protocols intersect when it comes to the censorship of transactions or protocol execution. Censorship of transactions occurs when protocols have a centralized intermediary but a

---

97. Schär, *supra* note 33, at 21.

98. Kaihua Qin, Liyi Zhou, Yaroslaw Afonin, Ludovico Lazzaretti & Arthur Gervais, *CeFi vs. DeFi—Comparing Centralized to Decentralized Finance*, *in* PROCEEDINGS OF ACM CONFERENCE (CONFERENCE '17) (2021).

99. *See, e.g.*, Securities Act of 1933, 15 U.S.C. § 77; Bank Secrecy Act, 12 U.S.C. §§ 1951-1960; Anti-Money Laundering Act of 2020, Pub. L. No. 116–283, 134 Stat. 3388; Investment Company Act of 1940, Pub. L. No. 117–263, 136 Stat. 2395; Investment Advisers Act of 1940, Pub. L. No. 117–263, 136 Stat. 2395.

100. Marco Dell'Erba, *Shadow Central Banking*, SSRN ELECTRON. J. 1, 3 (2019), https://ssrn.com/abstract=3488040.

101. Qin et al., *supra* note 98, at 3.

decentralized settlement system. In contrast, censorship of protocol execution relates to a centrally governed "DeFi" system—also encompassing CeFi ventures—which is what happens by employing certain types of cryptoassets such as stablecoins.[102]

DeFi's expanding list of services and products comprises asset exchanges, loans, stablecoins, decentralized governance voting, derivatives, and more. DeFi mostly offers products already existent in traditional finance.[103] Nevertheless, the choice of DeFi is grounded on the competitive higher annual percentage yield (APY), exceeding eight percent of interest.[104] In contrast, the ecosystem's opacity has also attracted financially inexperienced players who design products without a basic understanding of finance or financial regulation.[105] Inevitably, this has led to a crypto debacle over the last year.[106]

---

102. *See generally* Marco Dell'Erba, *Stablecoins in Cryptoeconomics: from Initial Coin Offerings to Central Bank Digital Currencies*, 22:1 N.Y.U. J. LEGIS. PUB. POL'Y 1 (2019). Stablecoins have a predominant role in DeFi. Stablecoins are cryptocurrencies (cryptoassets with a monetary function) that possess an economic structure allowing them to stabilize their price, usually pegged to another currency or an algorithm for stability. *Id.* at 7.

103. Qin et al., *supra* note 98, at 8.

104. Muyao Shen, *DeFi App Promising 20% Interest on Stablecoin Deposits Raises Concerns*, BLOOMBERG NEWS (Mar. 23, 2022, 3:37 PM), https://www.bloomberg.com/news/articles/2022-03-23/terra-s-promise-of-20-defi-return-raises-sustainability-concern?leadSource=uverify%20wall.

105. Declaration of John J. Ray III in support of Chapter 11 Petitions and First Day Pleadings, In re FTX Trading Ltd. et al., No. 22-11068-JTD (Nov. 17, 2022).

106. The common aspect of the 2022 debacles around DeFi have a common thread: centralization of processes and decisions despite their decentralization claims. LUNA (DeFi algorithmic Stablecoin) had significantly fewer transaction validators than its counterparts, with an accentuated centralization of operations—only 130 validators, as opposed to the 400,000 validators of the Ethereum Beacon Chain. Ahmed Ismail, *Luna's Collapse Shows DeFi's Dire Need for Technical, Regulatory Controls*, COINDESK: OPINION (May 12, 2022, 3:57 PM), https://www.coindesk.com/layer2/2022/05/12/lunas-collapse-shows-defis-dire-need-for-technical-regulatory-controls/ [https://perma.cc/3C74-PTB9]; Prashant Jha, *3AC: A $10B Hedge Fund Gone Bust with Founders on the Run*, COINTELEGRAPH (July 25, 2022), https://cointelegraph.com/news/3ac-a-10b-hedge-fund-gone-bust-with-founders-on-the-run [https://perma.cc/L2HG-UDQ3]. Celsius (a centralized finance lending platform), showed the vulnerabilities of DeFi's lending system by operating as a bank without maintaining the responsibilities that banks typically owe. Andrew Ross Sorkin et al., *Celsius Lays Bare Crypto Vulnerabilities*, Comment to *China's Shuddering Economic Engine*, N.Y. TIMES: DEALBOOK (July 15, 2022), https://www.nytimes.com/2022/07/15/business/dealbook/chinas-shuddering-economic-engine.html?searchResultPosition=1. Furthermore, the issues of centralized operations emerge among uncovered parent/sister cryptoenterprises. For example, Ooki Dao (Decentralized Autonomous Organization), an unincorporated association, was recently found liable for illegally offering leveraged and margined retail commodity transactions to their sister company, bZeroX. Press Release, Commodity Futures Trade Comm'n, *CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange*

A. Major Players

A commonly held belief is that DeFi is a transnational cross-border system without needing to trust anyone, forcing a distorted vision of a solo cryptoanarchist behind their own personal computer.[107] The assumptions of complete decentralization and disintermediation revealed the misconception that DeFi is a structureless system. Contrarily, any enterprise willing to transfer value and organize its economic activity cannot be removed from a formal structure.[108] To start, decentralization does not imply disintermediation. Even if DeFi enterprises are within the spectrum of decentralization, concentrated power still exists on blockchain. After the crisis of one of the major cryptoexchanges, there has been a great interest in uncovering the role of leaders in the venture and the enterprises supporting the system. The following is a brief account of major players on DeFi.

1. Coders

In a recent high-profile cryptoexchange bankruptcy case, the newly appointed CEO described the inefficiencies of the system he oversaw as failing any "corporate controls" guided by "a very small group of inexperienced, unsophisticated and potentially compromised individuals."[109] This depiction of cryptomarkets and their internal governance structure is interesting from different points of view.

The term coders is used interchangeably to define a wide range of protocol developers. While it is believed that the creator of Bitcoin was a solo participant, protocol developers belong to a non-homogeneous category.[110] Precisely, protocol developers in permissionless blockchains

---

Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act (Sept. 22, 2022), https://www.cftc.gov/PressRoom/PressReleases/8590-22 [https://perma.cc/WJ4Z-8RKY]; FTX/FTT (Centralized Exchange for cryptoassets), Executives from FTX's parent trading company misappropriated funds from investors, lenders and customers. Other financial mismatches are LBRY (Tokens)—recently found liable by the SEC for selling unregistered securities even though there was no ICO process—and non-fungible tokens (NFTs) acquired by cryptoenterprises and used as collateral in lending schemes.

107. May, *supra* note 1.

108. Zetzsche et al., *supra* note 89, at 181-98.

109. Declaration of John J. Ray III in support of Chapter 11 Petitions and First Day Pleadings, In re FTX Trading, Ltd., *supra* note 105, at 2.

110. NARAYANAN ET AL., *supra* note 3, at XXIII; Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A. Plummer & Nelson M. Rosario, *Blockchain Development and Fiduciary Duty*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 139, 183 (2019); Josh Lerner & Jean Tirole, *Some Simple Economics of Open Source*, 50 J. INDUS. ECON. 197, 200 (2002); DE FILIPPI & WRIGHT, *supra* note 5, at 97.

can be included in three macro categories: catalysts, open-source developers, and freelance coders.[111]

Catalysts act as founders of open-source projects or decentralized autonomous organizations.[112] Under a narrow vision of DeFi, catalysts/founders would eventually step out from governance roles.[113] However, it is possible that catalysts remain indefinitely behind the decentralized organization.

Open-source developers are unpaid coders or volunteers. They usually contribute to the code review after public disclosure and enhance trust in the project. Yet, there are also freelance protocol developers who are paid protocol developers hired by firms involved in the venture.[114]

Next to protocol developers are smart contract developers. Smart contract developers work on top of the protocol layer, building decentralized applications and smart contracts that are very important for DeFi. They create these accessible programs outside protocol developers' operations and control.[115] Smart contract developers usually create and deploy cryptoassets and DeFi applications on the Ethereum blockchain, even if there are other blockchains in the DeFi ecosystem, such as Cardano and Polkadot.[116]

Miners differ from coders. Miners work on the foundation layer, supporting the network through consensus.[117] As blockchain networks became popular, the number of miners increased, and with that, the level of difficulty of consensus protocol diminished the chances of getting a reward.[118] Miners are grouped in mining pools and act as a business

---

111. Different from protocol developers are smart contract developers, who build dApps and smart contracts. Their services aid the decentralized organization.

112. Haque et al., *supra* note 110, at 152.

113. Lerner & Tirole, *supra* note 110, at 221.

114. Haque et al., *supra* note 110, at 152.

115. DE FILIPPI & WRIGHT, *supra* note 5, at 27-28.

116. CARDANO, https://cardano.org/ [https://perma.cc/SDX5-V6QE]; Max Moeller, *Cardano-based DeFi Protocol Hopes to Incentivize Dapp Development*, COINTELEGRAPH (Jan. 25, 2022), https://cointelegraph.com/news/cardano-based-defi-protocol-hopes-to-incentivize-dapp-development [https://perma.cc/WJY7-MZG6]; POLKADOT, https://polkadot.network/ [https://perma.cc/7MYN-ESXK] (last visited Sept. 27, 2023); Danny Nelson, *Parallel Finance Launches DeFi 'Super App' for Polkadot Crypto Ecosystem*, COINDESK (Mar. 18, 2022), https://www.coindesk.com/tech/2022/03/18/parallel-finance-launches-defi-super-app-for-polkadot-crypto-ecosystem/ [https://perma.cc/6XNB-LLLR].

117. To avoid mining centralization, the Ethereum founders made their PoW consensus, Ethash, application-specific-integrated-circuits (ASIC) resistant, which makes it harder to process block transactions and having greater chances to receive a reward. ANDREAS M. ANTONOPOULOS & DAVID WOOD, MASTERING ETHEREUM 321 (O'Reilly Media ed., 2018).

118. Liyi Zeng Yang Chen, Shuo Chen, Xian Zhang, Zhongxin Guo, Wei Xu & Thomas Moscibroda, *Characterizing Ethereum's Mining Power Decentralization at a Deeper Level*,

organization, combining computational resources and operating costs to achieve economies of scale otherwise inaccessible. There is some opaqueness in their business model and operational activities, but it was estimated that before the PoS consensus, a handful of mining pools controlled more than fifty percent of the transactions on the Ethereum blockchain network.[119]

2. Decentralized Exchanges (DEXs) and Cryptoexchanges

DEXs are a class of on-chain asset exchanges where buyers and sellers of cryptoassets meet.[120] The DEX does not impose a specific exchange rate or follow any particular listing requirements comparable to stock exchanges. However, this illustration of a DEX as a mere marketplace ignores the constant absorption of financial business functions into one big player. Cryptoexchanges are an example of the exacerbation of vertical integration, simultaneously performing the roles of a marketplace, broker-dealer, and credit or lending activities provider.[121]

There is a misconception that all cryptoexchanges are decentralized exchanges. Certainly, they both have blockchain technological underpinnings in common, but cryptoexchanges are placed within the CeFi structure, namely in the spectrum of centralization. Indeed, cryptoexchanges are mostly custodial and managed by a team.[122] Still, recent problems with cross-border transactions involving cryptoexchanges identify some of their flaws, such as a lack of auditing or internal controls and a lack of oversight.[123] All these issues have put cryptoexchanges under increasing scrutiny.

DEXs are non-custodial exchanges. In other words, the user is in constant control of their funds. Moreover, DEXs possess specific trading characteristics.[124] Many DEX functions, such as automated market makers (AMMs), have been studied in algorithmic game theory but never

---

PROCEEDINGS—IEEE INFOCOM, at *1 (July 26, 2021), https://ieeexplore.ieee.org/document/9488812 [https://perma.cc/8M98-VXBE].

119. *Id.*

120. Humbel & Eckert, *supra* note 92.

121. Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz & William J. Knottenbelt, *SoK: Decentralized Finance (DeFi)*, ARXIV 1, 3 (Jan. 21, 2021), https://arxiv.org/abs/2101.08778 [https://perma.cc/Y32J-ZNLE]. For an overview of cryptoexchanges and vertical integration, see Marco Dell'Erba, *Crypto-Trading Platforms as Exchanges*, MICH. ST. L. REV. 1, 10 (2023).

122. Qin et al., *supra* note 98, at 6.

123. Dell'Erba, *supra* note 121, at 8.

124. Werner et al., *supra* note 121, at 3.

implemented.[125] Unlike their traditional counterparts, DEXs possess a level of automation that consents to a continuous flow of trading. With traditional order books, the matches between buyers and sellers were guided by the supply and demand of those assets.[126] In DEXs, all the transactions are settled on-chain. Thus, there is no pre- or post-liquidity trading.[127] Notwithstanding, increased automation opens the door to arbitrage trading. Arbitrage is used to facilitate the search for the best transaction fees, which in turn secure block allocation through a scheme called priority gas auctions (where gas is the fee paid in every transaction block).[128]

In contrast, the centralized nature of cryptoexchanges, just like stock exchanges, makes them subject to system outages. Moreover, the off-chain governance of cryptoexchanges sometimes reflects their lack of transparency because not all transactions are visible to members.[129] At the same time, the lack of internal controls or external audits may not necessarily result in liquidity issues but solvency ones.[130]

Nevertheless, DEXs suffer from other issues, such as middleware attacks and other AMM attacks.[131] Given the on-chain nature of DEX, a recurrent attack is observed on the underlying technology. In this sense,

---

125. *Id.*

126. Jiahua Xu, Krzysztof Paruch, Simon Cousaert & Yebo Feng, *SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols*, ARXIV 1, 3 (Mar. 23, 2021), http://arxiv.org/abs/2103.12732 [https://perma.cc/JHL8-UGQ4].

127. *Id.* at 1.

128. Claude Humbel, *Decentralized Finance: A New Frontier of Global Financial Markets Regulation*, 2022 GESKR 9, 15 (2022).

129. Dell'Erba, *supra* note 121, at 59.

130. The cryptoexchange FTX's crisis showed that without of proof of reserves, even an unfounded rumor is capable of incentivizing a run on the bank among their cryptoasset holders. Matt Levine, *FTX Had a Death Spiral*, BLOOMBERG, at *10 (Nov. 9, 2022, 2:10 PM), https://www.bloomberg.com/opinion/articles/2022-11-09/bankman-fried-s-ftx-had-a-death-spiral-before-binance-deal.

131. Xu et al., *supra* note 126, at 21. Besides middleware attacks, there are rug pulls (inducing people to buy worthless cryptoassets and swapping them for valuable ones, such as ETH), frontrunning (being the first trader to obtain the best cryptoasset price), backrunning (a detrimental attack on the network aimed at getting the block reward by beating a valid transaction with an invalid but simultaneous and longer one), sandwich attacks (a combination of frontrunning and backrunning where a trader searches for a pending transaction and places two order, thus manipulating cryptoasset prices), and vampire attacks ("stealing" users by giving them cryptoassets as an incentive to migrate to an exact copy of the existent platform). *Id.* The biggest vampire attack, perpetrated by SushiSwap, created a competing Uniswap-like platform, which produced a loss of $1.2 billion for the Uniswap trading platform. Connor Dempsey, *Vampire Attack! looksRare vs. OpenSea*, COINBASE, at *3 (Feb. 10, 2022), https://www.coinbase.com/blog/vampire-attack-looksrare-vs-opensea.

DEXs are frequently the target of middleware-layer attacks (an attack on the smart contract that operates as a bridge between complex transactions).[132] In addition, DEXs can also suffer an attack on the application layer, targeting lending products infrastructure or, in other words, manipulating oracles.[133]

3. Oracles

Oracles are certifiers of information in DeFi. They are third parties—humans or programs—that introduce external off-chain data from multiple external sources into the smart contract.[134] They perform a fundamental function in DeFi: enabling intra-transaction composability by ascertaining the conditions of complex smart contracts.[135] These data feeds access information through web scrapping, or information is inserted with other techniques.[136] Oracles have different applications, among them put options, insurance (e.g., introducing flight cancellation information), and regulatory compliance in digital assets sales on the Metaverse.[137]

One of the main oracle companies is Chainlink. Chainlinks's decentralized oracle network (DON) enhances DeFi protocols and applications by ensuring appropriate proof-of-reserves (PoR).[138] It can also work as a (decentralized) custodian when it comes to wrapped assets.[139] However, Chainlink's primary objective is to facilitate the transition of the traditional banking and monetary system into a digital

132. Xu et al., *supra* note 126, at 12.

133. *Id.* at 20.

134. Villanueva Collao & Winship, *supra* note 82, at 750.

135. The smart contract characteristic has also caused DeFi protocols to be called *Lego* projects, where a transaction is partitioned into multiple smart contracts as if they were small plastic bricks needed to connect or construct an object. In this case, a DeFi project. Schär, *supra* note 94, at 169.

136. Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels & Elaine Shi, *Town Crier: An Authenticated Data Feed for Smart Contracts*, CCS '16: PROC. 2016 ACM SIGSAC CONF. ON COMPUT. & COMMC'NS SEC. 270, 271 (2016).

137. The experiences on alternative virtual markets do not exempt the transnational regulations such as AML and know-your-customer (KYC) practices, which can be implemented through decentralized oracles. Joshua Tobkin, *The Metaverse Needs Oracles*, NASDAQ, at *2 (July 27, 2022, 10:00 AM), https://www.nasdaq.com/articles/the-metaverse-needs-oracles [https://perma.cc/TGP4-SCRR].

138. Lorenz Breidenbach et al., CHAINLINK 2.0: NEXT STEPS IN THE EVOLUTION OF DECENTRALIZED ORACLE NETWORKS, at *35 (Apr. 15, 2021), https://research.chain.link/whitepaper-v2.pdf [https://perma.cc/LNY2-CJ9L].

139. *Id.*

one by connecting blockchains with central bank digital currencies (CBDC) and authenticating or certifying the information.[140]

While China has already moved a step ahead in the development of digital currencies, the U.S. has not yet implemented measures for the creation of global payment systems.[141] The debate around private digital currencies centers around stablecoins (and similar assets) for fear of systemic risk, among other economic harms. However, discussions on creating norms for a competitive public-private digital money sector are still unfulfilled.[142] CBDCs and digital money would represent a shifting paradigm in global transactions because of the system's transparency, where all the transactions are theoretically traceable. With transparency, increased surveillance concerns would make fiat money more valuable because of the inherent privacy. Nevertheless, cryptographic advances in decentralized oracles (DECO) might protect users' confidentiality and prove the provenance of such data without revealing additional personal data.[143]

B. Decentralized Lending (DeLe)

Loans are an area of vital importance for commercial transactions and financial markets. Loans are acts of trust involving an assumption of risk among different parties. In commercial transactions, loans are enforced through legally binding contracts where one party, having an expectation of repayment, gives the other party credit—an act of confidence.[144] DeFi has changed loan assumptions of trust and confidence

---

140. *Id.* It is unclear how governments will characterize CBDC and how much blockchain technology will be necessary to achieve digital money serving as a legal tender or to show on-chain reserves or settlement accounts. Jiaying Christine Jiang & Karman Lucero, *Background and Implications of China's E-CNY,* 33 U. FLA. J. L. & PUB. POL'Y 237, 261 (2023).

141. DIGITAL CURRENCIES: THE US, CHINA AND THE WORLD AT A CROSSROADS at xxi (Darrell Duffie & Elizabeth Economy eds., 2022), https://www.hoover.org/research/digital-currencies-us-china-and-world-crossroads [https://perma.cc/F8RV-8KDC]; Thai-Binh Elston, *China Is Doubling Down on its Digital Currency*, FOREIGN POL'Y RSCH. INST., at *2 (June 2, 2023), https://www.fpri.org/article/2023/06/china-is-doubling-down-on-its-digital-currency/ [https://perma.cc/FH3S-2VW2].

142. *See generally* DIGITAL CURRENCIES: THE US, CHINA AND THE WORLD AT A CROSSROADS, *supra* note 141.

143. For an overview on DeCo, see Fan Zhang, Deepak Maram, Harjasleen Malvai, Steven Goldfeder & Ari Juels, *DECO: Liberating Web Data Using Decentralized Oracles for TLS*, CCS '20: PROC. 2020 ACM SIGSAC CONF. ON COMPUT & COMMC'NS SEC. 1919 (2020).

144. NOAH VARDI, CREDITWORTHINESS AND 'RESPONSIBLE CREDIT' 1-2 (Brill, 2022).

reposed on others through decentralized lending (DeLe).[145] In DeLe, decentralized platforms operate in permissionless blockchains, where both the lender and borrower do not need to know or identify themselves to conclude loan transactions (in other words, borrow or lend money and receive interest).[146]

In traditional finance, loans are secured through specific security agreements where the lender can foreclose, take possession, or control specified collateral in case of default.[147] In this sense, a security interest attaches to the collateral the debtor owns (or has acquired rights upon it) in exchange for the extension of credit—namely, the secured creditor has given value (consideration).[148]

DeLe loan operations are compiled in bytecode and deployed in blockchain through Protocols for Loanable Funds (PLF).[149] PLFs are protocols that help lending and borrowing activities in DeFi. PLFs create distributed ledger-based markets that pool cryptoassets—which form the collateral—in a smart contract.[150] PFLs differ from the Intermediation of Loanable Funds (ILF) model of banking because credit activities are programmatically enhanced through protocols. Thus, the agreement, provision of funds, and the collateral attachment occur directly in the same blockchain transaction. PLF aims to solve common issues in secured transactions, such as reneging debt commitments, defaults, secret liens, or priority issues. The collateral is directly liquidated through auctions automated with AMMs and sold on an exchange.[151]

---

145. Lewis Gudgeon, Sam Werner, Daniel Perez & William J. Knottenbelt, *DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency*, AFT 2020—PROC. 2ND ACM CONF. ADVANCES FIN. TECH. 92 (2020).

146. Schär, *supra* note 94, at 164.

147. U.C.C. § 1-201(b)(35) (Am. L. Inst. & Unif. L. Comm'n 2001). The UCC distinguishes security interests as secured positions created by contract from other types of liens, which are involuntary secured positions, such as statutory liens and common law liens.

148. U.C.C. § 9-203(b)(1)(Am. L. Inst. & Unif. L. Comm'n 2010). The consideration requirement implies that the creditor must give value to validate the seriousness of the promises and ensure perfection of the credit position. LYNN M. LOPUCKI, ELIZABETH WARREN & ROBERT M. LAWLESS, SECURED TRANSACTIONS. A SYSTEM APPROACH 134(8th ed. 2016).

149. Gudgeon et al., *supra* note 145, at 92.

150. Werner et al., *supra* note 121, at 4.

151. PLFs are not disintermediated platforms. On the contrary, they perform an intermediary function among platform users (borrowers and lenders). Gudgeon et al., *supra* note 145 at 92. The PLF model would have resembled the ILF model if banks were real intermediaries in credit transactions. Scholarship has showed that assets and liabilities in the IFL model do not reflect real assets or existing loanable funds, but the provision of financing function of banks, namely, banks' business model, which gravitates around the creation of money. Zoltan Jakab & Michael Kumhof, *Banks Are not Intermediaries of Loanable Funds—And Why this Matters*, at *2 (Bank of Eng., Working Paper No. 529, 2015) https://www.bankofengland.co.uk/working-

The same caveats related to language apply. Cryptolending is a general term encompassing all lending platforms using blockchain and DLT. However, cryptolending is within the spectrum of the CeFi/DeFi. Thus, there are cryptolending platforms with major centralized attributions, such as BlockFi, Celsius, and Gemini, as well as decentralized lending platforms, such as Compound, Aave, and dYdX.[152]

1. DeLe Protocols in DeFi

DeLe protocols show the true DeFi feature of intra-transaction composability, or money *Lego*, enhancing interoperability across DeFi project codes (or protocols/software) by allowing them to automatically connect like pieces of a Lego puzzle. For example, cryptoassets created or deposited in a specific lending protocol can be the capital source for a different protocol. Hence, these cryptoassets can be reused to secure a loan (used as collateral). Correspondingly, DeLe could be understood as a system of composable protocols reflecting cryptoassets and debt obligations.[153]

The interest rates are established using governance mechanisms and thus, decided at a protocol level rather than being set by central banks. Cryptoasset holders decide over interest rates using their governance tokens. However, this governance mechanism affects price volatility.[154] In DeLe, borrowers earn interest on PLF loans through margin trading of the collateral posted, profiting from the debt position. Consequently, borrowers engage in short selling, acquiring the debt position at a lower price later in time.[155]

PLF loans are divided into over-collateralized loans and flash loans.[156] In overcollateralized loans, the borrower provides cryptoassets

---

paper/2015/banks-are-not-intermediaries-of-loanable-funds-and-why-this-matters [https://perma.cc/99L6-QGT5].

152. GOFORTH & GUSEVA, *supra* note 14, at 610. Despite the custodial nature of the Compound protocol, scholars place it within the DeLe platforms. Kaihua Qin, Liyi Zhou, Pablo Gamito, Philipp Iovanoci & Arthur Gervais, *An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities*, PROC. ACM SIGCOMM INTERNET MEASUREMENT CONF. 336, 337 (2021).

153. Gudgeon et al., *supra* note 145, at 95.

154. *Id.* at 94.

155. *Id.* at 95.

156. Werner et al., *supra* note 121. This type of over-collateralization and lending has been observed in traditional finance through securitization. In securities financing transactions, collateral is represented by securities in exchange for other securities or cash loans. The lender gives the legal title of the securities, usually bonds, to the borrower (the one receiving and taking title over securities) in exchange for cash. The lender (the one receiving cash or other bonds)

as collateral to secure the transaction. The collateral must exceed the amount of the loan and is posted on a smart contract acting as an escrow account. The lender gives value, namely, provides cryptoassets for the exact amount of the loan, which is sent directly to the borrower's account.

Moreover, overcollateralized loans can be distinguished in collateralized debt positions (CDP) and collateralized debt markets (CDM).[157] In collateralized debt positions, platforms allow borrowers to issue new cryptoassets (stablecoins) by depositing a different one (such as ETH) on a locked account. The new cryptoassets represent a debt position and a collateralized loan.[158] This process is automated and does not require a counterparty. The protocol merely deploys the smart contract with the amounts pre-established and conditions introduced by oracles.

Collateralized debt markets (CDM) do not issue or create new stablecoins. On the contrary, CDM allows borrowers to resort to existing cryptoassets for lending operations. The lender deposits cryptoassets into the lending pool, and the borrower overcollateralizes the amount borrowed. Through this operation, borrowers also act as lenders every time the lending pool makes the collateral available for lending.[159] CDM offer fixed interest rates perfected and matured at the time of a peer-to-peer match between lenders and borrowers.[160] Additionally, CDM offer variable interest rates depending on the supply and demand of a lending pool. Thus, earnings start when the lender gives value by depositing the funds into a pool (a smart contract), but the liquidity (availability of funds) of the lending pool determines the interest rates.[161] As a result, in times of scarcity, the lending interest rates are higher and thus profitable for lenders.

---

transfers legal title for a limited time and is obliged to reinvest the cash received. In this case of lending against cash, this securities financing transaction is called repo-lending or repurchase agreement. Arvind Krishnamurthy, Stefan Nagel & Dmitry Orlov, *Sizing Up Repo*, 69 J. FIN 2381, 2386 (2014). Repo-lending was a central factor in the 2008 financial crisis. Paradoxically, overcollateralization in DeLe works in a similar way.

157. Schär, *supra* note 94, at 164-65.

158. *Id.* at 164. The number of cryptoassets (stablecoins) representing collateralized loans created/issued from this process depends on price parameters, the exchange rate of the crytpoassets locked against the new cryptoassets (stablecoins), and the ratio between locked and newly issued stablecoins. Frequently, the ratio of cryptoassets locked represents 150% more than the amount borrowed.

159. Qin et al., *supra* note 98, at 7.

160. Schär, *supra* note 94, at 165.

161. *Id.*

2. Flash Loans

These positions are called uncollateralized—using non-legal terminology—even if flash loans are secured positions. In these types of transactions, the liquidity provider (lender) supplies the funds while having *control* over cryptoassets. The lender exercises control through flash loans embedded into smart contracts with annexed conditions and a cycle for repayment.[162] Any borrower willing to pay the fee for the transaction is potentially an eligible borrower. Thus, creditworthiness is assessed in spite of any credit score history. At the end of the cycle, the borrower has to repay the amount lent plus interest, and in case of default, the transaction is automatically reversed. This reversal implies that the on-chain state remains unmodified.

Because there is no synchronization among different exchanges, once the transaction is reversed, the same cryptoassets can have different prices depending on the exchange. As a result, this scenario encourages the exploitation of price differences or arbitrage. Flash loans also pose different types of cryptomarket risks, such as inflation of trading volume (wash trading), "instant swapping from one collateral to another" (using AMMs), and "variation of flash loan[s]."[163] Furthermore, flash loans consent to fast access to a massive amount of cryptoassets (governance tokens). However, access to a large amount of concentrated capital in DeFi carries many downsides. Precisely, concentrated capital determines a new way of manipulating the ecosystem with attacks, affecting governance.[164] Certainly, flash loans are not the cause of the attacks but are the vehicle for governance attacks with minor skin in the game.[165]

The automation of secured transactions using blockchain led the path to the Uniform Laws Commissioner's exploration of a new Chapter 12, where the perfection of a secured transaction (agreement) can occur with control over electronic registered records.[166] Moreover, the

---

162. Werner et al., *supra* note 121, at 4.

163. Kaihua Qin, Liyi Zhou, Benjamin Livshits & Arthur Gervais, *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*, FIN. CRYPTOGRAPHY & DATA SEC.: 25TH INT'L CONF. 3, at 8 (2021), http://dx.doi.org/10.1007/978-3-662-64322-8_1 [https://perma.cc/FK3Q-6A6T].

164. Werner et al., *supra* note 121, at 7.

165. Qin et al., *supra* note 98, at 8.

166. The approach of Chapter 12 is technology-neutral, but it seeks to address emerging issues with cryptoassets. It remains for the single states to adopt Article 12. Frank Emmert, *Cryptocurrencies: The Impossible Domestic Law Regime?*, 70 AM. J. COMPAR. L. 185, 204-09 (2022). *See* UNIFORM COMMERCIAL CODE AND EMERGING TECHNOLOGIES, AMENDMENTS TO THE UNIFORM COMMERCIAL CODE, https://www.uniformlaws.org/committees/community-home?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac [https://perma.cc/TUS7-YEA4].

emphasis on cryptoassets' control in flash loans might have an impact on the application of embedded judicial remedies such as replevin and a progressive dismissal of self-help remedies. Furthermore, the transparent nature of DeLe on-chain transactions eases the filing requirements for perfection and priority.[167]

3. Liquidations

At the fulfillment of certain conditions, liquidators are able to sell the locked collateral on an exchange. The conditions are not relegated to mere default but also to cryptoassets decrease in value through automated deleveraging. Secured creditors are less worried about the form of the collateral but more about its value.

For example, in collateralized debt positions, when the collateral falls below a predefined threshold, the borrower receives part of the collateral at a discounted valuation to reduce exposure.[168] Indeed, the loan is available for liquidation by a smart contract, or the collateral can be liquidated through an auction.[169] Likewise, the debt can be rescued by adding collateral (topping up) and re-establishing its value conditions prior to its decrease. Finally, the borrower can redeem its default by repaying the debt manually.[170]

Due to high-interest rates, incentives to extend loans are soaring with consequent disinterest in saving.[171] This aspect of putting capital in circulation marks the development and expansion of different DeLe protocols, an expansion that traditional finance has not achieved. However, the DeLe development is not guided by governmental or transnational financial regulation, which, in some instances, creates illiquidity risks. For example, in traditional finance, trading of financial assets is limited over a fixed period of time to avoid affecting asset prices in lending. In DeLe, some protocols allow for immediate withdrawal of principal and interest, which leads to illiquidity periods and cryptoasset price volatility.[172] Moreover, high interest rates can incentivize borrowers

167. Carla L. Reyes, *Creating Cryptolaw for the Uniform Commercial Code*, 78 WASH. & LEE L. REV. 1521, 1533-34 (2021).

168. Gudgeon et al., *supra* note 145.

169. Qin et al., *supra* note 152, at 339.

170. *Id.* However, this option has been revealed as impractical even when some automation is added since avoiding losses requires control of collateral price and fees.

171. Gudgeon et al., *supra* note 145, at 97.

172. Humbel, *supra* note 128, at 15.

to default, having the same illiquidity effects but affecting lenders (liquidity providers) since they cannot withdraw their funds.[173]

Moreover, in times of financial crisis—when the price of cryptoassets falls—overcollateralization does not eliminate the risk of ending up with an underwater debt.[174] In other words, the borrower could end up not paying the debt to avoid losses since the collateral is worthless (meaning that at the end of the loan, the borrower would not receive back the cryptoassets posted as collateral).

C. Derivatives

Derivatives are contracts to transfer risk. This risk depends upon or is derived from a set of underlying assets whose value changes as market variables of those assets move. The risk lies in the unfulfillment of a future promise, known as counterparty credit risk. As a result, derivatives allow the risk one party does not want to bear to be transferred to another in exchange for a fee.[175]

In traditional finance, the market for derivatives is divided into bilateral private contractual agreements (over-the-counter (OTC)) and exchange-traded derivatives. Centralized intermediaries (broker-dealers or exchanges) handle the different transaction phases of securities and derivatives. Thus, they decide the circumstances that allow transaction confirmation, clearance, and settlement.[176] All of this information is managed in centralized ledgers that need to be constantly updated across intermediaries.

OTC derivative trades are commonly based on personal relationships involving dealers. Building a trusting relationship between dealers (or other professionals) and their clients is necessary to mitigate settlement and counterparty credit risk.[177] Nevertheless, since the agreements are made privately, OTC trades lack transparency in ascertaining derivatives' real value (price) or the parties involved.[178]

In contrast, in exchange-traded derivatives, market participants are aggregated and meet at exchanges with standardization of processes, but

---

173. Gudgeon et al., *supra* note 145, at 97.

174. Werner et al., *supra* note 121, at 9-10.

175. DAVID MURPHY, DERIVATIVES REGULATION 9 (2022). Futures and options are among the most common derivative contracts.

176. DE FILIPPI & WRIGHT, *supra* note 5, at 95.

177. MURPHY, *supra* note 175, at 22.

178. DE FILIPPI & WRIGHT, *supra* note 5, at 92. The issues related to the opaque nature of OTC derivative trades led to the 2008 financial crisis as many financial institutions engaged in asset-backed securities and collateralized debt obligations that were eventually unfulfilled.

there is great competition across exchanges.[179] As a result, derivatives trading benefits from centralized monitoring and management through central counterparties (CCP), as well as enhances price discovery and favorable risk transfer.[180] Each derivative counterparty is replaced with a CCP to protect the trade from default—in other words, assigning or novating the contract to the CCP. CCPs have a series of requirements and standards developed by the associated exchange practice. The CCP annexed standards have diminished the costs of posting collateral through multilateral netting.[181] Indeed, exchanges and CCPs maintain clearinghouses and require that participants provide funds posted as collateral before joining to avoid defaults.[182] This market structure has determined the domestic nature of the exchange-traded derivatives with standards and rules that limit compliance to the internal market. In contrast, the OTC market structure, which consists of private agreements, allows transnational operations.[183]

Yet, derivative transactions involve numerous risks, such as market risk, counterparty credit risk, settlement risk (when trading in foreign exchanges), and funding and market liquidity risk.[184] Increased regulation aimed at mitigating those risks has raised the standards for market participants, making derivative activities costly.

Blockchain technology has modified this process. Its transaction settlement attributes facilitate derivatives trading. Moreover, the convergence of specific protocols makes it possible to create decentralized derivatives whose value arises from an underlying set of assets or a specific event, among other variables.[185]

There are two main types of decentralized derivatives: (1) synthetic (and its derivation of inverse synthetic) and (2) event-based derivatives.

1. DeFi Synthetic Assets

Synthetic assets are asset-based derivative tokens whose price is extracted from a cryptoasset's performance. These synthetic cryptoassets

---

179. MURPHY, *supra* note 175, at 23.

180. Albert J. Menkveld & Guillaume Vuillemey, *The Economics of Central Clearing*, 13 ANN. REV. FIN. ECON. 153 (2021).

181. *Id.* at 164-65. In multilateral netting, the CCP manages the defaults, and all participants can net their risks from trades on the exchanges, regardless of the initial counterparty before the novation. *Id.*

182. DE FILIPPI & WRIGHT, *supra* note 5, at 90.

183. MURPHY, *supra* note 175, at 25.

184. *Id.* at 18.

185. Schär, *supra* note 94, at 166. Those assets include fiat currency, commodities, cryptocurrencies, index funds, etc.

replicate off-chain/real-world assets on-chain. By opening a collateralized debt position, a DeLe platform is not restricted to the issuance of stablecoins (cryptoassets pegged to a fiat currency or other cryptoasset), but extended to other types of synthetic cryptoassets.[186] Thus, instead of having a CCP managing the trading and settlement of positions, the counterparty will mint synthetic derivatives, mirroring the economic properties of other assets without requiring the issuer to hold that asset. However, the report of external prices or changes in risk is incorporated through oracles (such as Chainlink). Thus, oracles ease asset tracking through smart contracts-based price discovery protocols.[187] A prominent example of synthetic assets is developed by the Synthetix protocol, a platform allowing the trading of perpetual futures (contracts to buy or sell an underlying asset without a specific delivery date) and spot Synth.[188] These synthetic assets (derivatives) can be deposited on other platforms/exchanges to provide liquidity and earn interest.[189]

A strand of synthetic derivatives is inverse synthetic derivatives in DeFi. These types of DeFi derivatives work through an inverse function of the original derivative, reflecting an inverse price of the underlying asset.[190] Thus, if the price of the underlying asset goes down or underperforms, these types of derivatives increase in value. These inverse derivatives give short exposure in crypto and the same payoffs as short positions in traditional finance.

2. DeFi Derivatives

DeFi derivatives are event-based derivatives, where a cryptoasset reflects an observable variable with a future but limited set of outcomes, such as political election results, eventually resolved at a specified period of time. These types of DeFi derivatives perform a similar function to collateral against derivatives exposure. Instead of posting cash or a portfolio of securities, the party must post cryptoassets as collateral into a smart contract, commonly 1 ETH. In exchange, the party receives a

---

186. *Id.* at 166-67.

187. Synthetic assets perform differently from tokenized commodities, namely crytpoassets reflecting commodities. Tokenized commodities are backed by the incorporated assets. In this sense, the person owning the tokenized commodity must own the underlying asset. In comparison, synthetic assets allow trading of the underlying asset without owning it. *Id.* at 157-58, 166.

188. *Synthetix Litepaper*, SYNTHETIX (Jan. 2023), https://docs.synthetix.io/synthetix-protocol/the-synthetix-protocol/synthetix-litepaper [https://perma.cc/KAP2-C2JF].

189. Gudgeon et al., *supra* note 145.

190. Schär, *supra* note 94, at 166.

set of sub-tokens (cryptoassets) representing all the potential outcomes, where each outcome imbued in the cryptoasset is traded separately.

These event-based derivatives are the foundation for prediction markets in DeFi, where oracles—the only external source introducing off-chain elements—leave these platforms vulnerable to protocol attacks. Different from traditional derivatives, DeFi event-based derivatives introduce resolution systems that correct conflicting pricing information and act as an alternative arbitration court with members voting for an agreed outcome.[191]

Blockchain implementation in derivatives has reduced market conditions such as information asymmetries and the lack of transparency, especially in OTC trades. At the same time, it has impacted the derivatives market structure, expanding it to cross-border participants. Nevertheless, decentralized derivatives and the protocols that constitute them are not clearinghouses.[192] Thus, decentralized derivatives lack an important aspect of CCPs: insurance against counterparty risk.[193] The mutualistic nature of CCPs protects the derivatives market against systemic risk. Hence, in case of default, the system has enough funds to cover those costs.[194] However, in DeFi and synthetic derivatives, the default of a large financial player can halt the entire ecosystem.

V. CONCLUSION

Web 3.0 has gained considerable recognition due to the introduction of the Ethereum blockchain, connecting dispersed nodes with smart contracts. The legality or *alegality* of these technological instruments is an irrelevant question for operators in this area that blatantly ignore the corpus of regulation around capital markets.[195] Indeed, developers have built thousands of infrastructures and a decentralized market of unlimited participants interacting in a unique ecosystem known as decentralized finance (DeFi). This aggregation of protocols and applications consents to the technological distribution of financial services.

However, not all financial services in DeFi are genuinely decentralized. Rather, they are placed within the spectrum of centralization and decentralization (CeFi and DeFi), introducing several

---

191. *Id.* at 167. Augur is one of the leading platforms dealing with prediction markets.

192. Paolo Saguato, *The Unfinished Business of Regulating Clearinghouses*, 2020 COLUM. BUS. L. REV. 449, 451 (2020); Schär, *supra* note 94, at 97.

193. Saguato, *supra* note 192, at 451; DE FILIPPI & WRIGHT, *supra* note 5, at 97.

194. Menkveld & Vuillemey, *supra* note 180, at 159.

195. Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Alegality of Blockchain Technology*, 41 POL'Y & SOC. 358 (2022).

issues. Cryptoassets play a fundamental role in this area but do not have a coherent body of regulation since the current regulatory apparatus seems too antiquated to accommodate these digital assets together with the conflicting idea of a private monetary system.

The ability of blockchain to allow the settling of transactions programmatically has influenced the sprout of new protocols and applications for loanable funds. Crypto exchanges commonly offer these options within their cryptoassets trade services, but there are other platforms specialized solely in lending products. These platforms do not aim to substitute the bank's role in the credit system. They instead offer the possibility to access credit without any credit score history or even without collateral. Creditworthiness is obtained by posting collateral or by electronic control of the amount borrowed. The loan options are divided into collateralized or uncollateralized loans. However, both types of lending protocols are technologically secured transactions.

The issues that arise from the unregulated, transnational, and technological system of DeFi center around the pseudonymity of its participants, the opacity of the business models, and the lack of auditing or external code controls. All these issues affect potential investors and consumers of these products while leaving the door open for systemic risk issues. Even if blockchain purports to eliminate intermediaries and to distribute or decentralize access to capital, the examination of the DeFi ecosystem shows otherwise. In particular, it highlights a concentration of assets that may facilitate attacks on protocols with the ambition to manipulate governance.

DeFi has many downsides in its current state, but the technology is still in its infancy. An efficient cryptomarket is yet to come, but the technological potential is promising to legal scholars since economic phenomena have always been attracted to the domain of law.