Decentralized Finance

Subjects: Business, Finance
Contributor: Giulio Caldarelli

The term Decentralized Finance (DeFi) refers to an alternative financial infrastructure built on top of public blockchains. DeFi uses smart contracts to create protocols that replicate existing financial services in a more open, interoperable, and transparent way Source.

Keywords: blockchain ; decentralized finance ; oracles ; smart contracts

1. DeFi Applications

Decentralized Finance (DeFi) is proving to be one of the most significant use-cases for public blockchains, with over fifty billion dollars of value locked and growing [1][2]. DeFi already offers a wide variety of applications such as Stablecoins, Derivatives, Decentralized exchanges, and Decentralized lending. A brief description of those is provided hereafter.

1.1 Lending Pools (Decentralized Lending)

Not to be confused with Liquidity Pools; lending pools are financial applications that create a crypto-asset loan market. Managed by a system of smart contracts and incentive mechanisms, they create advantages for lenders as well as for borrowers [3]. Loans are an essential part of the financial ecosystem, and in the DeFi platforms, it is possible to lend and borrow crypto assets without KYC procedures [4]. Users can lend their assets to the LPs, and receive an LP token which serves as a sort of receipt of their lending. The LP tokens can then be transferred, and their exchange negotiated like any other token allowing for a sort of crypto securitization of the loan [5]. However, if the token is lost or stolen, the amount lent will also be forfeited.

It is important to note that the main risk for a lender is that a borrower could run away with the money (crypto), and it is crucial in an environment in which the borrower cannot be identified. There are two mechanisms that aim to solve this problem:

Collateralized loans are loans given after the borrower locks a predetermined amount of assets. Usually, the locked amount should exceed the borrowed amount. The smart contract then decides the ratio between collateral and the borrowed amount and the interests to be paid. Of course, in order to recover the locked assets, it is sufficient to refund the loan [4]. Due to the fact that those loans run on a decentralized system, there is no way to renegotiate terms after its execution, and if the contractor is unable to repay the debt, the collateral is liquidated (sold at a discounted rate). Although P2P lending exists, the most common lending type is organized in pools of which Compound, Aave, and dYdX are among the leading dApps [6][7][8].

Flash loans are a particular form of loans that are only possible thanks to the implementation of smart contracts. The name was coined by Max Wolff, the creator of Marble protocol, in 2018 [9]. It consists of a particular form of contract in which the loan is taken and repaid simultaneously [10]. That way, the illiquidity, and the default risks are denied. In a globalized crypto market, flash loans are beneficial when performing arbitrage. An investor can borrow an amount of money to buy the crypto from a market, sell them in a market where the price is higher and repay the loan making a profit. All can and should happen in transactions within the same block. Since the loan is taken and repaid simultaneously, there is virtually no limit to the amount of money borrowed (subject to availability of the requested token).

Oracles in lending pools and flash loans are important to determine the price of assets and, in particular, to those held as collateral. The value of a deposited digital asset determines the amount of loan that can be borrowed, and for lenders, the interest that has to be accrued. Unlike Aave and dYdX that outsource oracle-related tasks to Chainlink, Compound has its own price oracle [11][12][13]. Oracles on Compound are managed by administrators, who are COMP token holders. The administrator deploys a price aggregator contract in which it specifies *min*, *anchor,* and *tolerance* sets. The *min* is the minimum number of reports necessary to calculate a new median value. The *anchor* is the address of the contract that

requires the price feeds. Finally, the *tolerance* is the maximum deviation accepted by the contract, which is usually set at 10%. Price oracles on Compound protocol could be represented by major exchanges, other DeFi projects, and Over-the-Counter (OTC) services. If the reports are under the min or if the median value calculated by the aggregator exceeds the tolerance, the value is rejected, and the asset's price will not be updated [14][15]. If oracles fail to provide the right collateral price for lending contracts, there is the risk for it to be under-collateralized. That poses severe threats for the lender to recover the investment if the borrower cannot repay the debt. In flash loans, oracle failures are even more dangerous as they can even damage the whole platform.

1.2. Automated Market Makers (AMM)

Automated Market Makers, often referred to as decentralized exchanges, are smart contracts that hold both assets of a trading pair. For example, in the case of ETH/USDT, the smart contracts hold a certain amount of Ether and Tether in what is called a liquidity pool [16]. The price of each asset is derived as a function of availability and, of course, is stabilized by arbitrage. Unlike centralized exchanges, the companies that manage AMMs, have the role of developing contracts, minimize the chance of bugs and malfunctions, but they do not directly provide the assets [17]. The fees paid in the exchange are then shared among the liquidity providers and service providers. Uni-swap, pancake-swap, and just-swap are the most known AMMs in the respective ecosystems: Ethereum, BinanceSmartChain, and Tron [18]. It is important to point out that, as stated by Schär [4], smart-contract-based liquidity pools do not rely on price oracles to operate. According to the author, the product model of a liquidity pool can be expressed as XY = K in its simplest form. Where x and y are the token reserves and k is a constant. If an agent wants to buy Δ′ coins of token "y" must put in the swap contract, enough "x" such that the product of the reserves remains constant. Angeris [19] formalize this concept with the following function:

$$(R' - \Delta')\,(R + \Delta) = R'\,R$$

Furthermore, the price of assets is derived with a similar principle. It is constantly adjusted so that if the asset X is deposited to take Y, then the price of Y raises, as it will be less and less convenient to keep buying the same asset. That way, it would be indeed profitable the opposite swap (deposit Y to take X) so that the pool should never be drained. Despite not relying on oracles or exchanges to price their assets, liquidity pools, thanks to that mechanism, are sometimes more efficient than centralized exchanges in determining the price of assets. For that reason, DEXes are often selected as price oracles. Uniswap, for example, is being lately chosen as a reliable price oracle by Aave, bZx, Debank, and others [20]. Consequently, the developers have implemented specific features to serve that particular purpose [21]. The Uniswap price oracle evolved, in fact, from V1 to V2, changing from the last swap price feed to a time-weighted average price feed. While the first offered chances for flash-loan attacks, the second type was less exploitable with flash loans. More technically, while with the V1, every token transacted price was registered in the block and immediately used as a feed, with the V2 version, the feed is extracted as a mean value of 24-h transactions for that specific rate [22]. It is essential to notice that, although liquidity pools do not require oracles to operate, they expose the liquidity providers to the risk of "Impermanent Loss" [23]. This risk arises when one asset significantly changes its price with respect to the other in the contract. This provides an opportunity for arbitrageurs to drain the asset unbalancing the pool. Given the lack of one of the assets, when the LP provider withdraws its liquidity, it will then receive an amount with a lower value than that provided, experiencing a "permanent" loss [24]. Given the seriousness of the issue, lately, platforms such as Bancor are implementing oracles to limit the action of arbitrageurs. On the other hand, other approaches such as the one followed by Balancer include the chance to provide assets also with an unbalanced rate (e.g., 40/60, 90/10, etc.)

1.3. Stablecoins

To better exploit the advantages of the new financial services offered by DeFi, it is crucial to rely on means of exchange with a stable value [25]. Unlike common cryptocurrencies (e.g., Bitcoin and Ethereum), which are extremely volatile, stablecoins maintain almost constant value over time. Stablecoins are usually pegged to the value of an external asset such as gold, but a majority are linked to the US Dollar. Depending on how the system is linked to the stable value, different kinds of stablecoins can be distinguished.

Custodial stable coins are crypto-assets whose stable value is guaranteed by an external authority. The most known stable coins are Tether (USD-T) and USDC, which mainly operate on Ethereum blockchain and are managed respectively by Tether Operations and Centre Organization [26][27]. Companies that manage stablecoins are generally in charge of guaranteeing the asset's value by the deposit (through a bank or another trusted entity) of the equivalent in dollars, gold, or other financial assets [25]. For example, to mint one million dollars of USDC, the same amount in dollars or assets must be locked within the trusted entity. Those stable coins are recognized as crypto assets in the sense that they can actively interact with other cryptocurrencies through smart contracts and exchanges, but like fiat currencies, their use can be

censored, seized, and limited by the issuing authority [28]. By definition, custodial stable-coins require trust in an institution that guarantees the pegs to a certain asset. For that reason, blockchain oracles are not required to derive the price of custodial stable-coins. On the other hand, market congestions or downturns may determine temporary deviance from the pegged value.

Non-custodial collateralized stable coins are crypto-assets whose value is not guaranteed by a centralized entity and, most of the time, are managed by a Decentralized Autonomous Organization [14]. DAI is, for example, a non-custodial stable-coin whose value is guaranteed by the deposit of a collateral (mainly Ethereum) whose volatility is exploited to stabilize the value of the asset. For example, after the deposit of $150 of ETH in the appropriate smart contract, it is possible to mint $100 of DAI. If ETH rise in price, then more DAI are minted to stabilize their value. On the other hand, if ETH price decreases, a proportional amount of DAI is burnt [29]. Unlike custodial stable-coins, non-custodial are open and censorship-resistant, but due to the over-collateralization rules (usually 150%), the total issued amount is generally lower [28]. Other examples of non-custodial stable-coins are sUSD and USDJ. Non-custodial stable coins, being untied by external entities who guarantee the asset's value, require oracles to verify the exchange rate between the stable coin and the collateral. Surely, the most interesting case is the MakerDAO Oracle. As extensively explained in Gu et al. [30], the MakerDAO oracle had a major change for which it can be distinguished in V1 and V2. In MakerDAO V1, the collateral for DAI stable-coin was only ETH, so that the oracle had to update ETH/DAI price in real time to enforce the collateralization ratio properly. The Maker V1 Governance whitelisted 14 independent, and anonymous price feeds "to monitor the reference prices across a number of external sources" [31]. When the DAI/ETH price is to be updated, a price oracle calls a function that indicates *value*, *valid_unitl*, and *medianizer.addr*. The *value* is the DAI/ETH claimed exchange rate, the *valid_until* indicates its expiration time, and *medianizer.addr* is the contract address of the *medianizer*. The *medianizer* then aggregates all the value from the price feeds. Of course, the *medianizer* updates the prices independently on when it receives the prices from the feeds, so it happens that aggregators use price feeds with different expiration times.

The MakerDAO V2, on the other hand, brought many innovations to the Maker Protocol. First, it enabled a multi-collateral feature. Second, it counts on a broader source of price feeds [32]. Unlike V1, in this new version, the identities of price oracles are disclosed (0x, dYdX, and Gnosis), and the contract also introduces a novel *medianizer* mechanism. The new protocol requires the presence of an Oracle Security Module (OSM) for each collateral type. In addition to the V1 functions, a poke function is introduced, which excludes feeds that lack three critical requirements [33]. First, feeds should be provided by a minimum number of sources. Second, the values should be all positive and presented in ascending order. Finally, signatures must be verified and belong to all different whitelisted feeds.

Non-custodial algorithmic stable-coins constitute a complex experiment in which the pegged value is not ensured by collateral but relies only on a system of algorithms and smart contracts [34]. Those projects employ a model in which the token holder receives new coins when demand increases. On the other hand, if the demand decreases, the amount is automatically deducted from the market to limit the loss of value. Although simple in principle, algorithmic stable coins are challenging projects to realize, and some, such as Basis, already shut down due to regulatory hurdles [35]. Ampleforth is a project which is still active and employs the algorithmic principle; however, the stability of its value still represents a challenge [36]. Ampleforth utilizes a system of oracles trusted by the platform that reports price feeds cyclically. The platform administrator sets min, delay, and expire parameters, where min is the minimum number of reports. Delay indicates the time from which the reports can be used and expire the time in which the report becomes unreliable.

CeloUSD is another algorithmic stable coin that implements a quite complex oracle type [37]. Celo protocol has a smart contract called SortedOracles that recognizes only four trusted price sources (Binance, Bittrex, Coinbase, and OKCoin). The Celo Oracle data aggregator, other than deploying the mean value, also checks if a minimum number of exchanges were queried [38]. The reporter then transfers the feed from the aggregator to the SortedOracle contracts, ideally on a stable time basis. For example, if the maximum age of a report is 5 min and there are ten participating oracles, then, every 30 s, an oracle should send a report. Celo also employs a "MetricCollector" that checks on the performance of oracles to detect anomalies in their behavior. The most attractive feature of Celo oracle is the so-called "Circuit Breaker". The circuit breaker basically shut down the oracle service in case of high volatility. Once shut down, the system should be restarted manually and revised by the platform expert before being operative again. During the shutdown, a trusted provider will adjust the price dynamically until the oracle restarts [39].

1.4. Derivatives

As known, derivatives are financial assets that derive their value from represented assets' performance [40]. Derivatives in DeFi are extremely important due to the lack of interoperability between blockchains. As Larsen [41] explains, "Bitcoin can't

speak the language of Ethereum and vice versa". This means that we cannot spend bitcoin on the Ethereum network, and we cannot operate Ethereum smart contract on the bitcoin network. Wrapped tokens were specifically made to overcome this limitation, in particular for DeFi applications. WBTC, as an example, is an ERC-20 version of bitcoin and can be spent on the Ethereum network and managed by Ethereum smart contracts. In order to issue WBTC on Ethereum, an equal amount of BTC has to be locked on the Bitcoin blockchain. An oracle service should then ensure that as long as WBTC is used on the Ethereum network, the corresponding amount on the bitcoin network is not spent. Being WBTC traded for other tokens and used as collateral for loans, failure in communicating the exact quantity of locked tokens can be fatal [41]. Due to the complexity of derivative contracts, their management is mainly left to centralized exchanges (Coinbase, Poloniex) [28]. Lately, however, some platforms such as Synthetix are also offering DeFi solutions in the derivatives field [42]. In those platforms, it is possible to find tokens representing all sorts of fiat currencies (such as GBPN representing Pounds), stocks or other crypto assets (wrapped tokens). The price of external assets offered on Synthetix is determined through a system of oracles provided through Chainlink. However, the requirements of Synthetix platforms are that the oracles should be distinct for each asset and that prices are updated every 5 or 10 min.

Universal Market Access (UMA) is another recently born platform that aims to create fast, efficient, and secure derivatives on the Ethereum platform [30]. Unlike Synthetix, it has its own oracle system made of two distinct modules called Optimistic Oracle and Data Verification Mechanism (DVM), respectively. UMA's oracles are not mandatory to use in principle, but if the contract needs a secure price feed, it can quickly require it with the Optimistic Oracle [43]. This oracle is mainly automated and provides an off-chain price feed within a pre-defined length of time, without the need to pay any on-chain fees. If the price is disputed, then the second UMA's oracle, the DVM, comes into play. The DVM works mostly like the Tellor and Razor oracle systems, and it takes two days to solve a dispute. Those who misreport price lose their bond in favor of those who reported a correct price. It is also possible to require a price directly to the DVM, but it will take two days to resolve anyway. UMA's whitepaper is also interesting because it has an appropriate section in which they explain how they claim to solve the oracle problem. They explain that if the price of the contract is high, then the oracles may be incentivized to provide imprecise price feeds for personal purposes. In particular, they distinguish between Profit-from-Corruption (PfC) and Cost-of-Corruption (CoC). The Cost-of-Corruption is the total amount of UMA tokens needed to perform a 51% attack on the platform. The Profit-from-Corruption is the total asset value of the derivative for which the price is requested. The UMA protocol then requires that the CoC is always greater than 200% of the PfC. In that way, although possible to perform a 51% attack, it will always be unprofitable. However, according to their website, this prevention system is not yet automated [44]. Furthermore, collusion is not the only risk of using oracles in DeFi.

2. Oracles and the oracle problem in DeFi

The blockchain oracle problem refers to the inability to determine the veracity of data provided by oracles [45]. The uncertainty may arise from an unreliable data source, low oracle reputation, or both [46]. However, as discussed in a recent paper [47], the consequence of this condition varies according to the specific sector in which blockchain is implemented. In the supply chain, the oracle problem refers to the fact that information collected on the blockchain is filtered by the producing company so that unwanted or sensitive information may not be registered [48][49]. In the academic sector, the oracle problem does not affect the authenticity of the transcript but does question the credibility of the issuing authority [50]. A certified issue by a low-ranked university, in fact, will not gain more credibility for being stored on a blockchain [51]. In the IPRs field, the oracle determines a more social problem in which authors and certification authorities are vying for the role of the oracle, as the one who does, obtain a greater power over the other party [52]. In resource management, since the data flow is bi-directional, namely when resources are both stored and shared, there is the need for two types of oracles (inbound and outbound). This further dependency, of course, doubles the problem. Finally, in the case of health records, the oracle involvement can constitute an additional attack vector for hackers to steal or modify patient records. When multiple oracles and external databases are implemented, and there is the inability to monitor their security actively, it will also be impossible to determine the reliability of patient's data on the blockchain [53].

Decentralized finance, as a real-world application, requires oracles to operate. However, the impact of their implementation strictly depends on the extrinsic data required. In DeFi, data such as KYC are not required (at the moment), since smart contracts manage all the transactions, and no centralized authority supervises the identity of the contractors [28]. Therefore, oracles are not implemented to collect personal data. Consequently, no GDPR or security issue arises, and no external server is needed for sensitive data management [54]. The only data that remain transparent are the transactions that only belong to pseudonym addresses.

Unlike the academic sector and IPRs management, a smart contract's authorship is guaranteed solely and exclusively by the private key that signs the agreement. Theoretically, whether the person who uses the private key is the legitimate owner of the wallet or not is not relevant for the correct execution of a DeFi contract [55][46]. Since not regulated through a

KYC procedure, there is no way to enforce an unwanted operation on a crypto wallet. On the other hand, as the application is decentralized, there is also no authority to appeal. The last thing to consider to narrow the oracle involvement in DeFi environment is the fact that those applications are meant to communicate with each other (interoperability) so that data flow in both directions. This creates similar issues as those found in blockchain applications for resource management (dual oracle problem) [56].

Regardless of the specific decentralized financial application, the only data required pertains to financial assets' quantity and price. Unlike the data production of a traced bottle of wine, asset data constitute publicly available knowledge that can easily be verifiable. Oracles based on the wisdom of the crowd should then be able to "trustlessly" fetch this sort of data. However, malfunctions, tampering, and collusion can still easily alter the data provided. Being financial contracts that often manage transactions of millions of dollars also dramatically affects the incentive to alter the communication channel [57]. Thus, despite the fact that the asset data are publicly available knowledge, there are still many issues that can prevent correct information from being registered on the chain. We could argue that the oracle problem in DeFi applications, from a theoretical point of view, reflects the chance for asset data to be altered by a malfunction or deliberately manipulated for selfish purposes.

References

1. Huilgolkar, H. Designing the Most Secure Oracle for the Decentralized Finance. Available online: https://medium.com/coinmonks/designing-the-most-secure-oracle-for-the-decentralized-finance-9853237f0c37 (accessed on 11 January 2021).
2. DefiPulse DexGuru-Real-Time Data. Analytics and Trading for AMMs in One Place. Available online: https://defipulse.com/blog/dexguru/ (accessed on 19 April 2021).
3. Bartoletti, M.; Chiang, J.H.; Lluch-Lafuente, A. SoK: Lending Pools in Decentralized Finance. arXiv 2020, arXiv:2012.13230.
4. Schär, F. Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets. FRB St. Louis Rev. 2020.
5. Harwick, C.; Caton, J. What's holding back blockchain finance? On the possibility of decentralized autonomous finance. Q. Rev. Econ. Financ. 2020.
6. Boado, E. AAVE Protocol Whitepaper. Available online: https://github.com/aave/protocol-v2/blob/master/aave-v2-whitepaper.pdf (accessed on 2 April 2021).
7. Leshner, R.; Hayes, G. Compound: The Money Market Protocol. White Paper. 2018. Available online: https://www.digitalcoindata.com/whitepapers/compound-whitepaper.pdf (accessed on 2 April 2021).
8. Juliano, A. dYdX: A Standard for Decentralized Margin Trading and Derivatives. 2018. Available online: https://whitepaper.dydx.exchange (accessed on 2 April 2021).
9. Qureshi, H. Flash Loans: Why Flash Attacks Will Be the New Normal. Available online: https://medium.com/dragonfly-research/flash-loans-why-flash-attacks-will-be-the-new-normal-5144e23ac75a (accessed on 19 August 2020).
10. Wolff, M. Introducing Marble: A Smart Contract Bank. Available online: https://medium.com/marbleorg/introducing-marble-a-smart-contract-bankc9c438a12890 (accessed on 12 March 2021).
11. Chainlink The Aave Oracle Network Powered by Chainlink Is Now Live! Available online: https://chainlinkecosystem.com/ecosystem/aave/ (accessed on 2 April 2021).
12. DYdX dYdX Chooses Chainlink as its Oracle Provider for New Market. Available online: https://integral.dydx.exchange/dydx-chooses-chainlink-as-its-oracle-provider-for-new-market/ (accessed on 2 April 2021).
13. Tiwari, A. DeFi Protocol Compound (COMP) Releases Decentralized Price Oracle. Available online: https://btcmanager.com/defi-protocol-compound-comp-decentralized-price-oracle/ (accessed on 5 April 2021).
14. Liu, B.; Szalachowski, P.; Zhou, J. A First Look into DeFi Oracles. arXiv 2020, arXiv:2005.04377.
15. Omelchenko, D. Compound Launches Decentralized Price Oracle. Available online: https://ihodl.com/topnews/2020-08-09/compound-launches-decentralized-price-oracle/ (accessed on 2 January 2021).
16. Wang, Y. Automated market makers for decentralized finance (DeFi). arXiv 2020, arXiv:2009.01676.
17. Leybold, M. Decentralized Finance (DeFi) in 2020 and Its Future Trajectory. Available online: https://www.linkedin.com/pulse/decentralized-finance-defi-2020-its-future-trajectory-matthew-leybold/ (accessed on 12 March 2021).

18. Coin Market Cap Coin Market Cap-Defi. Available online: https://coinmarketcap.com/view/defi/ (accessed on 5 April 20 21).
19. Angeris, G. When Is Uniswap a Good Oracle? Available online: https://medium.com/gauntlet-networks/why-is-uniswap-a-good-oracle-22d84e5b0b6c (accessed on 2 April 2021).
20. Enclave Projects Utilizing Uniswap Oracle. Available online: https://enclaveresearch.com/projects-utilizing-uniswap-oracle/ (accessed on 5 April 2021).
21. Waas, M. Using the New Uniswap v2 as Oracle in Your Contracts. Available online: https://soliditydeveloper.com/uniswap-oracle (accessed on 2 April 2021).
22. Angeris, G.; Kao, H.T.; Chiang, R.; Noyes, C.; Chitra, T. An analysis of Uniswap markets. arXiv 2019, arXiv:1911.0338 0.
23. Lielacher, A. What Is Impermanent Loss? Available online: https://trustwallet.com/blog/what-is-impermanent-loss (acce ssed on 3 April 2021).
24. Jakub What Is Impermanent Loss? DEFI Explained. Available online: https://finematics.com/impermanent-loss-explaine d/ (accessed on 13 April 2021).
25. Klages-Mundt, A.; Harz, D.; Gudgeon, L.; Liu, J.Y.; Minca, A. Stablecoins 2.0: Economic Foundations and Risk-based Models. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies; Association for Computing Machinery: New York, NY, USA, 2020; pp. 59–79.
26. Tether. Tether: Fiat Currencies on the Bitcoin Blockchain. Available online: https://assets.ctfassets.net/sdlntm3tthp6/SevuOTDbYiCcoaeKEoQAO/828cba8e4e76f9c3075594a98ba807df/TetherWhitePaper.pdf (accessed on 3 April 2021).
27. Centre USDC Centre whitepaper. Self-Published White Paper.; 2018.
28. Zetzsche, D.A.; Arner, D.W.; Buckley, R.P. Decentralized Finance (DeFi). IIEL Issue Brief 2020.
29. Coinbase DAI Stablecoin. Available online: https://www.coinbase.com/it/earn/dai (accessed on 9 April 2020).
30. Gu, W.C.; Raghuvanshi, A.; Boneh, D. Empirical measurements on pricing oracles and decentralized governance for stablecoins. SSRN Electron. J. 2020.
31. Maker Team the Dai Stablecoin System. Whitepaper. 2017. 21p. Available online: https://makerdao.com/whitepaper/DaiDec17WP.pdf (accessed on 9 April 2020).
32. Maker Introducing Oracles V2 and DeFi Feeds. Available online: https://blog.makerdao.com/introducing-oracles-v2-and-defi-feeds/ (accessed on 14 February 2020).
33. Maker MakerDAO Oracle Module. Available online: https://docs.makerdao.com/smart-contract-modules/core-module (accessed on 7 April 2021).
34. Harvey, C.R.; Ramachandran, A.; Santoro, J. DeFi and the Future of Finance; John Wiley & Sons: New York, NY, USA, 2021.
35. Al-Naji, N. Basis. Available online: https://www.basis.io/ (accessed on 5 April 2021).
36. Kuo, E.; Iles, B.; Cruz, M.R. Ampleforth: A New Synthetic Commodity. Ampleforth White Paper. 2019. Available online: https://www.ampleforth.org/papers/ (accessed on 7 April 2021).
37. Slawson, A. CELO Holders: Make Your Voice Heard through On-Chain Governance. Available online: https://medium.com/celoorg/celo-gold-holders-make-your-voice-heard-through-on-chain-governance-96cb5a1e8b90 (accessed on 7 April 2021).
38. Croessmann, R. Zooming in on the Celo Expansion & Contraction Mechanism. Available online: https://medium.com/celoorg/zooming-in-on-the-celo-expansion-contraction-mechanism-446ca7abe4f (accessed on 3 April 2020).
39. Celo-org Celo-Oracle. Available online: https://github.com/celo-org/celo-oracle (accessed on 7 April 2021).
40. Hull, J.C. Options, Futures and Other Derivatives, 1st ed.; Pearson Education India: New York, NY, USA, 2017; ISBN 9 781292212890.
41. Larsen, A. A Primer on Blockchain Interoperability. Available online: https://medium.com/blockchain-capital-blog/a-primer-on-blockchain-interoperability-e132bab805b (accessed on 9 December 2019).
42. Brooks, S.; Jurisevic, A.; Spain, M.; Warwick, K. Synthetix: A decentralised payment network and stablecoin v0.8. 2018.
43. UMA. UMA: A Decentralized Financial Contract Platform; UMA: New York, NY, USA, 2018.
44. UMA. How UMA Solves the Oracle Problem. Available online: https://docs.umaproject.org/oracle/econ-architecture (accessed on 3 April 2021).

45. Low, K.F.K.; Mik, E. Pause the blockchain legal revolution. Int. Comp. Law Q. 2020, 69, 135–175.
46. Antonopoulos, A.M.; Woods, G. Mastering Ethereum—Building Smart Contracts and DAPPS; O'Reilly Media, Inc.: Newton, MA, USA, 2018.
47. Caldarelli, G. Understanding the Blockchain Oracle Problem: A Call for Action. Information 2020, 11, 509.
48. Caldarelli, G.; Rossignoli, C.; Zardini, A. Overcoming the blockchain oracle problem in the traceability of non-fungible products. Sustainability 2020, 12, 2391.
49. Kumar, A.; Liu, R.; Shan, Z. Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities. Decis. Sci. 2020, 51, 8–37.
50. Sztorc, P. The Oracle Problem. Available online: https://www.infoq.com/presentations/blockchain-oracle-problems (accessed on 3 March 2020).
51. Caldarelli, G.; Ellul, J. Trusted academic transcripts on the blockchain: A systematic literature review. Appl. Sci. 2021, 11, 1842.
52. Finck, M.; Moscon, V. Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. IIC Int. Rev. Intellect. Prop. Compet. Law 2019, 50, 77–108.
53. Caldarelli, G. Blockchain Oracles and the Oracle Problem, 1st ed.; Amazon Publishing: Seattle, WA, USA, 2021; ISBN 979-1220083386.
54. Arndt, T. Towards an Implementation of Blockchain-Based Transcripts with Nosql Databases. In Proceedings of the 17th International Conference on E-Society 2019, Utrecht, The Netherlands, 11–13 April 2019; IADIS Press: Lisbon, Portugal, 2019; pp. 309–312.
55. Amler, H.; Eckey, L.; Faust, S.; Kaiser, M.; Sandner, P.; Schlosser, B. DeFi-ning DeFi: Challenges & Pathway. arXiv 2021, arXiv:2101.05589.
56. Mühlberger, R.; Bachhofner, S.; Castelló Ferrer, E.; Di Ciccio, C.; Weber, I.; Wöhrer, M.; Zdun, U. Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World. In Proceedings of the International Conference on Business Process Management; Springer: Cham, Switzerland, 2020; pp. 35–51.
57. Frankenreiter, J. The Limits of Smart Contracts. J. Inst. Theor. Econ. JITE 2019, 175, 149–162.
