Decentralized Finance, Stablecoins, and Macroeconomic Stability

Rohit Shetty

September 30, 2021

rshetty23@gmail.com

If you like this piece and would like to donate some BTC, you can do so here:

12FHkULMQpQjuiLXFW9qiYgKeHT4grApQd

For my TradFi folks, PayPal at the above email address also works

Table of Contents

Introduction ***3***

Markets ***5***

Lending **5**

Variable Rate 5

Fixed Rate 6

Decentralized Exchanges **6**

Automated Market Makers 6

Demand Aggregators 8

Synthetics **8**

Options **9**

Perpetual Swaps **10**

Collateralized Loan Obligations **11**

Asset Managers **12**

Supply Aggregators 12

Traditional Managers 12

ETFs / Index funds **13**

Collectively Organized 13

Individually Customized 13

Stablecoins & Macroeconomic Stability ***14***

Money and Its Creation **14**

Attempts at Macroeconomic Stability **15**

Attempts to Combat Systemic Risk **15**

Concerns of the Fed & Regulators **16**

Types of Stablecoins **16**

Vulnerabilities with Stablecoins **17**

Likely Stablecoin & Regulatory Policy **18**

Facebook's Diem: The Dollarization of Developing Economies **19**

Central Bank Digital Currencies **19**

Appendix: Virtual Worlds ***21***

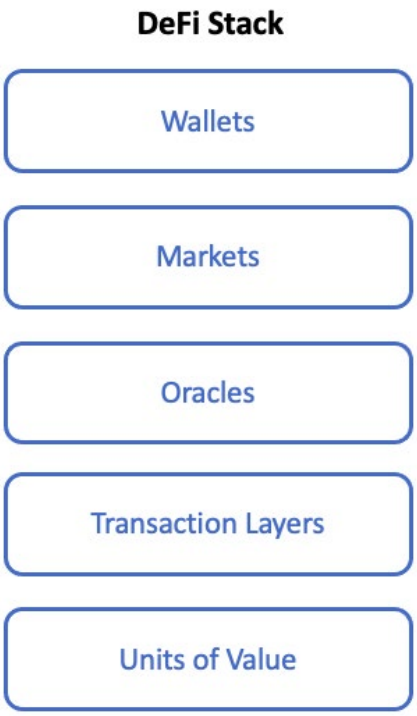
Endnotes ***22***

Introduction

Decentralized Finance

Decentralized finance (DeFi) operates in a completely permissionless manner without third parties (e.g., companies or governments) being able to block trades or collect fees. This occurs via smart contracts, which are pieces of code that specify the terms of a trade and then automatically execute a transaction according to those terms. These contracts and their outcomes exist in a transparent manner across a distributed blockchain that no single entity can control (i.e., it is censorship resistant).

The DeFi Stack



Within that context, a simplified version of the DeFi stack can be seen to the right[1]. Across layers of the DeFi stack and within any given layer, different applications can interact with each other because they are composable. Composability means that the output of one building block can be used as the input of another building block. This allows the various components to interact and build off of each other, opening up all sorts of creative possibilities.

Units of Value

Units of value are what you start the DeFi process with and what you anticipate getting back to a greater degree at the end. Units of value typically involve stablecoins, which are meant to hold their value against the U.S. dollar. Examples of stablecoins include Tether, USD Coin, Binance USD, Dai, and TerraUSD, among others. This paper will go into more detail on stablecoins later on. Other units of value may include cryptocurrencies such Bitcoin (BTC) and Ethereum (ETH). [2]

As a general note, this paper will focus primarily on: 1) Units of Value, and 2) Markets. The other layers of the DeFi stack (Transaction Layers, Oracles, and Wallets) will only be dealt with briefly.

Transaction Layers

Transaction layers are Layer 1 solutions that allow applications with smart contracts to be built on top of them. Ethereum was the first Layer 1 solution to allow for smart contracts. Developers can create applications using the Solidity programming

language and execute those applications using the Ethereum Virtual Machine. While Ethereum can handle a maximum of 30 transactions per second and often has high gas fees (which are needed to make transactions go through), there are Layer 2 solutions being built on top of it, such as the Optimism and Arbitrum rollups. [3] With these solutions, transactions would execute more quickly on Layer 2 and only settle on Layer 1 (Ethereum) later on. These Layer 2 solutions will roll out fully sometime later this year. Over 90% of current decentralized exchange volume is through Ethereum. [4]

Another Layer 1 solution is Solana, which uses proof of history[5] to precisely timestamp each transaction, so that the transactions can be stitched together later on in the right order by the various nodes. This, along with other innovations, have allowed Solana to process up to 65,000 transactions per second. However, the network is more centralized since it is newer and the hardware requirements for running a node are more demanding.

Oracles

An oracle is a third party which provides on-chain smart contracts with the external off-chain information needed to execute those contracts (e.g., the price of BTC is necessary for a related options contract). The effectiveness of a smart contract rests heavily on its access to accurate information, and most oracles seek out data from many different sources to ensure such accuracy. Chainlink is the most popular decentralized oracle, though Pyth's use is growing quickly.

Markets

DeFi markets will be covered in much more detail later in this paper. However, such markets include:

1) Lending: variable rate, fixed rate
2) Exchanges: automated market makers, demand aggregators
3) Derivatives: synthetics, options, perpetual swaps, collateralized loan obligations
4) Asset Managers: supply aggregators, traditional
5) ETFs / Index Funds: collectively organized, individually customized

Wallets

Crypto wallets keep your digital assets safe by storing your private keys. A hardware wallet allows for cold storage (i.e., it is not connected to the internet so there are fewer attack vectors). Online wallets involve storage of private keys in an app or via software. Metamask is the most popular online wallet used with decentralized exchanges, though many others exist.

Markets

I won't keep repeating it, but for all of these markets, please keep in mind that everything described here happens in a completely programmatic manner via smart contracts, without any ongoing third-party involvement in the trades. Everything is organized and executed on the blockchain using software.

Lending

Variable Rate

Most lending related to digital assets involves variable interest rates. Compound is an example of a variable rate lender. In Compound, depositors can deposit stablecoins, ETH, or ERC-20 tokens. [6] In return, the depositor receives cTokens. For example, if DAI is deposited then the depositor would receive cDAI in return. If ETH is deposited, then cETH would be received. These cTokens can be returned to Compound at any point in exchange for the original underlying asset plus the interest accrued. Interestingly, these cTokens can also be sold or traded on the open market. [7] Depositors also receive Compound's governance token, COMP, which fluctuates in price.

On the borrowing side, the identity and creditworthiness of potential borrowers is not known. Instead, borrowers are required to overcollateralize their loans. Borrowers may provide collateral that is of a different type than what they borrow in (e.g., they could provide ETH as collateral but borrow DAI). There is a collateralization ratio that ranges from 0 to 1. Liquid large cap coins have a higher collateralization ratio (e.g., 0.75) and more illiquid small cap coins have a lower ratio (e.g., 0.4). A user's borrowing capacity is the market value of their collateral multiplied by the collateral ratio.

As an example, say $100 worth of ETH is deposited as collateral with a collateralization ratio of 0.75. In that case, total borrowing capacity is $75. A user's borrowing capacity may be breached if: 1) the value of the collateral drops, and/or 2) the value of the coin that was borrowed rises. Borrowers have the option to increase their collateral or pay down their loan so that they stay within their borrowing capacity.

However, if the borrower breaches its borrowing capacity, then third party arbitrageurs are allowed to purchase a portion of the underlying ETH collateral at a slight discount. The borrower keeps the amount that was loaned to it, but Compound receives the cash from the ETH collateral sale (i.e., the borrower loses some of its collateral). From Compound's perspective, this reduces its risk tied to that borrower.

Compound determines the depositor rate and borrowing rate for any given asset type (e.g., DAI) based on the supply and demand for that specific asset. [8, 9] These

variable borrowing and lending rates adjust with each new Ethereum block, so borrowers could see rates jump on them. [10] Compound currently has $15.6bn in deposits while Aave, a competitor, has $19.1bn in deposits. [11]

Fixed Rate

Fixed rates on crypto lending are also available. In traditional finance, bonds can be separated out into their periodic coupon payments (strips) and their final repayment of par value (zero coupon bonds). Similarly, Element Finance accepts deposits of ETH, BTC, USDC, or DAI, and then deposits that amount in a vault (e.g., say that it is 10 ETH). The contents of the vault are then invested for a fixed time period (say 6 months) through a platform like Compound or Aave, and the initial depositors are given Element principal tokens (10 epETH) and Element yield tokens (10 eyETH). The principal tokens will return the face value of 10 ETH at the maturity of the contract, and the yield tokens will pay all returns over those 6 months minus that final par payment of 10 ETH. The epETH is akin to a zero coupon bond, and the eyETH is a strip. Since the epETH will return par in 6 months, it will trade at a discount to its par value in the present with an implicit fixed interest rate associated with that asset type (in this case, ETH). For example, the 10 epETH might be worth 9.8 ETH in the present, implying a fixed annual interest rate of 4.1%.[12] In contrast, eyETH will accrue the value of the average variable rate over the next 6 months. However, instead of holding onto the eyETH, an investor might sell it in the present and use the proceeds to purchase epETH, so that only a fixed rate is received on the initial investment. [13, 14]

Implicit Interest Rate Swaps

In contrast, "yield compounding" involves selling the epETH and using the proceeds to purchase eyETH. This transforms the entire investment into only yield without any payment of par value at the end. The previous two actions (only holding epETH or only holding eyETH) appear analogous to an interest rate swap. If you only hold epETH, you are implicitly paying the variable rate on ETH in order to receive the fixed rate on it. However, if you only hold eyETH, you are implicitly paying the fixed rate in order to receive the variable rate.

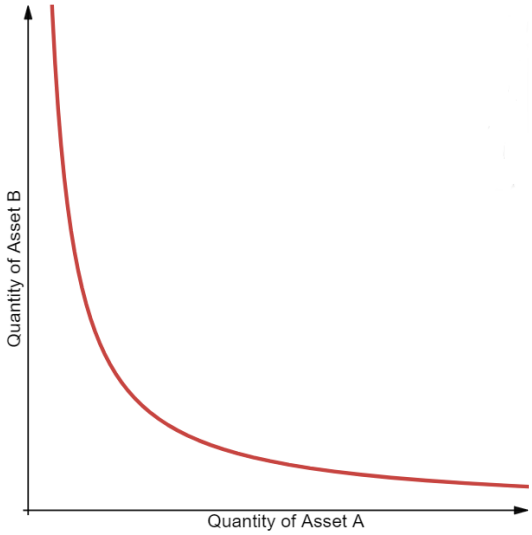
Decentralized Exchanges

Automated Market Makers

Traditional exchanges match buyers and sellers directly through a central order book model. If either side of a trade lacks liquidity, then exchange-affiliated market makers are obligated to take that side of the trade. While some decentralized exchanges use a central order book model, our focus here will be on automated market makers (e.g., Uniswap).

Automatic market makers (AMMs) create a market for each cryptocurrency pair. Let's take ETH/DAI as an example. To start a liquidity pool, the initial investor would deposit the same dollar amount of ETH and DAI in the pool. For example, say that ETH is trading at $2000/ETH. If 50 ETH are deposited in the pool, then that is worth $100,000, and so 100,000 DAI must be deposited in the pool at the same time. If this is happening on Uniswap, then anyone who wants to trade this pair on Uniswap can do so through this pool. The initial exchange rate of DAI/ETH will be the same as the market rate (since $100,000 of each was provided). If the initial exchange rate is not set at the market rate, then arbitrage relationships exist (e.g., if the rate is too low, then ETH can be bought from the pool and sold elsewhere for a profit; and if the rate is set too high, then ETH can be purchased elsewhere and sold to the pool for a profit).

AMMs operate using a constant product rule. In our example above, there are initially 50 ETH and 100,000 DAI. This multiplies to 5,000,000. Any subsequent trades would have to keep the product of the amount of ETH and the amount of DAI constant. For example, if someone on Uniswap wants to purchase 1 ETH, then that would leave 49 ETH in the pool. Since the product must be constant at 5,000,000, that means that the amount of DAI after the trade occurs must be: (5,000,000)/49 = 102,040.82. Since the pool previously had 100,000 DAI, then the cost to the Uniswap user to purchase 1 ETH would be 2040.82 DAI (this comes from 102,040.82 – 100,000). The difference of ~40 DAI from the initial exchange rate is referred to as slippage and is explicitly stated for each Uniswap trade before an order is confirmed. The slippage here is ~2%.



However, consider a larger initial trade of 10 ETH (instead of the 2 ETH trade). That would have left 40 ETH in the pool, and so there would need to be 125,000 DAI to keep their product constant at 5,000,000. This means that those 10 ETH would be exchanged for 25,000 DAI at rate of 2500 DAI/ETH. The slippage here is much higher at 25%.[15] In general, the smaller a trade is relative to the size of the liquidity pool, the lower the slippage rate. The opposite is true if a trade is quite large relative to the liquidity pool. In the graph to the right, you can see how the exchange rate (represented by the slope of the curve) changes based on the amount of each asset held. [16] In general, if an exchange rate differs too greatly from that of other markets, arbitrageurs will help bring things back in line (in the manner mentioned above).

For the initial liquidity pool, if a second person had wanted to invest in the liquidity pool, then they would have contributed ETH and DAI at the same 2000 DAI/ETH exchange rate. For example, if they had contributed 10 ETH and 20,000 DAI, then pool would have had 60 ETH (from 50 + 10) and 120,000 DAI (from 100,000 + 20,000). In this case, the constant product would have been 7,200,000 (from 60 * 120,000). From there, things would have operated

similarly. In general, the liquidity providers receive LP tokens based on how much liquidity they provide a particular pool. Trades are executed with a 0.3% trading fee, and this revenue goes to the LP token holders of that pool. Some AMMs also provide liquidity providers with governance tokens for the exchange, so that the overall process is known as liquidity mining.[17]

This example is for one cryptocurrency pair on Uniswap (ETH/DAI), but such liquidity pools exist for every pair offered on the platform. If a certain pair is not offered, then you can achieve your end through routing. For example, if you want to trade BAT/GRT but there is no direct liquidity pool for it, then two trades (BAT/ETH and ETH/GRT) can be automatically executed to get you there.

Uniswap is the largest AMM, though PancakeSwap and SushiSwap also have high volume. Curve Finance uses a unique algorithm to make sure that related cryptocurrency pairs trade closer to each other. [18] Interestingly, Balancer is an AMM that allows for liquidity pools with up to 8 tokens. [19]

Demand Aggregators

Demand Aggregators like the 1Inch Exchange simply aggregate all of these AMMs so that a trader can immediately find and execute on the best price for a given trade across the whole ecosystem. Other demand aggregators include Matcha, Dex.AG, and Paraswap.

Synthetics

Synthetics are derivatives which mirror the price movement of an underlying asset. The Mirror Protocol allows synthetic mAssets (e.g., mXAU for XAU or gold) to be created via overcollateralization. The necessary overcollateralization to mint a new mAsset is 150% when the collateral is made up of stablecoins, and it is 200% for all other collateral types. [20] An oracle tracks the price of the underlying asset (e.g., gold in this case), and an increase in the mAsset price may require the minter to provide more collateral to maintain the necessary collateralization ratio. If the collateralization ratio is breached, then the Mirror protocol will seize a portion of the collateral and use it to purchase and burn the related mAsset. This reduces the Mirror protocol's liability as there are now fewer mAssets outstanding. The protocol does this at the cost of the minter, since part of its collateral was sold. Apart from this, if a minter wants to free up its collateral, it must return the mAsset to the protocol, at which point it is burned.

Arbitrage relationships help keep the mAsset price in line with the price of the underlying asset. For example, say that XAU is $100, but mXAU has recently traded down from $100 to $90. If someone had previously minted mXAU at $100 and sold it, they can now purchase mXAU at $90, return it to the Mirror protocol, free up their collateral by burning that mXAU, and then

pocket the $10 difference. Burning mXAU reduces its supply, which increases its price. This continues to happen until mXAU rises back to $100. [21]

On the other hand, say that mXAU has recently traded up from $100 to $110, despite XAU being $100. In that case, an arbitrageur can mint mXAU at $100 (per the oracle), immediately sell it for $110, and keep $10 in profit. This increases the supply of mXAU and causes its price to fall. This process continues until mXAU falls from $110 back down to $100.

In general, synthetics allow you to immediately start trading many different kinds of assets on the blockchain without having to store or transfer the underlying asset.

Options

European call options give you the right to purchase an asset at a particular price (the strike price) at a specified time. In contrast, European put options give you the right to sell an asset at a particular price at a specified time. [22] In the past, options on BTC and ETH had to be fully collateralized. This means you had to set aside the entire amount of BTC or ETH that was needed, if you were writing a call option (so that this BTC/ETH could be delivered in whole if the option were exercised), or you had to set aside the dollar amount of a put's strike price (so that you would be able to purchase the underlying asset at this price if need be). This is safe, but it is not capital efficient. [23]

Opyn is a platform for writing and purchasing options that only requires partial collateralization. It does this through a system of margining for individual option writers. Opyn might determine the necessary margin through scenario analysis by asking: 1) "If the spot price moves 25% against the option writer, what would be the intrinsic value of the option if exercised?"; and 2) "What would be the value of an ATM option at the new lower spot price, assuming implied volatility of 350% and an interest rate of 40%?". These two values (the exercise value of the option with a price shock and the time value of the option at the shocked price) are then added. This is the margin that option writers must maintain at all times to not have their position liquidated. This required level of margin adjusts continuously based on the changes in the spot price. The numbers mentioned here are just an example, as Opyn's governance mechanism determines the exact parameters.

If an option writer breaches its minimum margin level, then a reverse Dutch auction is used to liquidate the options that it wrote. Opyn will offer higher and higher prices to buy back the options that were written by that issuer until all of those positions have been cleared from the market. Both call and put options on BTC and ETH are sold and margined in the manner described here. [24]

Perpetual Swaps

A swap is a derivative that exchanges the cash flows and liabilities associated with two different financial assets. A perpetual swap is a swap that continues forever. If a swap is entered against USD or a stablecoin, then one is essentially going long or short the other asset (e.g., BTC). Perpetual protocol enables swaps between any kind of crypto. However, trades are both initiated and settled in USDC.

The notional value of swaps are often much larger than the amount of margin initially offered up. For example, you could put down 100 USDC in margin and take a long position in ETH that is worth 1000 USDC. Perpetual allows you to take on up to 10x leverage at position initiation, and this can rise to 16x (if the position goes against you and your margin gets cut) before your margin will begin to be partially liquidated.

Interestingly, Perpetual protocol employs a virtual AMM that operates very similarly to the AMMs mentioned above in the "Exchange" section. However, the vAMM is purely virtual, so no assets actually enter it. Instead, the swap's notional value (e.g., long 10 ETH against USDC) is entered into the vAMM purely as an ongoing simulation. The liquidity pools in the vAMM operate exactly as described before, with a constant product rule that helps determine the price of the asset that is being purchased (in this case, ETH). The simulation continues when other swap positions are initiated or closed.

Funding payments are used to make sure that the exchange rate of a crypto pair in the vAMM stays close to its spot price. For example, with ETH/USDC, if the price of ETH is too high versus spot, then the individuals who hold long ETH swap positions have to transfer a funding payment from their margin to the participants who have on a short ETH/USDC swap position. The opposite would occur if the price of ETH/USDC is lower than spot. This incentivizes people to increasingly take the side of the trade that helps bring the virtual exchange rate back to spot. Arbitrageurs might do this and also offset their Perpetual swap position by holding the opposite position at another exchange. This allows them to collect the funding payments while waiting for the two prices to converge. [25]

As mentioned before, if losses accrue and cause the net margin to fall to than 6.25% of the notional value of the swap (i.e., if there is more than 16x leverage), then 25% of the loss suffered thus far will be crystallized. During this process, the notional value of the trade will also be cut (with the size of this reduction tied to the constant product rule). The notional value of the swap will fall by a greater percentage than the margin does, pushing the margin ratio back above 6.25%.[26]

In general, Perpetual protocol allows people to gain quick access to a leveraged crypto position, though one must be mindful of margin requirements and potential liquidations.

Collateralized Loan Obligations

Collateralized loan obligations pool together a group of loans and then tranche out the returns from those loans. For example, the senior tranche may receive a low return but it would also have first right to the revenue stream coming in from those loan payments, making it a safer investment. The mezzanine tranche would have second right to the revenue stream of loan repayments (as this tranche only receives money if the senior tranche is paid first), but it would provide a higher return to compensate for the additional risk. Equity tranches have last right to the revenue stream, but they also offer the highest returns, since they represent the residual after everyone else has been paid. They also suffer the first loss.

Barnbridge's SMART Yield Bonds introduce CLOs to digital assets by: 1) taking in money from investors; 2) depositing this capital at lending platforms like Compound, Aave, and Maker; and 3) then tranching out the variable rate loan payments that it receives. The senior tranche makes up 70% of the initial capital invested, while the junior tranche consists of the remaining 30%. The senior tranche may offer a low but safe 5% return, while the junior tranche could return over 20% (Scenario 1), though it will also suffer first losses (Scenario 2). [27]

This product allows investors to select the risk/return bundle that would most appeal to them. Since this is done through smart contracts, all of the individual underlying loans as well as the platforms that they reside on are completely transparent to investors. Each tranche's tokens are freely traded allowing investors to enter, exit, or switch between tranches as they wish.

Though not a CLO, Barnbridge's SMART Alpha Bonds tranche out the volatile returns of an underlying crypto asset (e.g., ETH). Senior tranches receive a more muted return on the crypto asset (e.g., half of the profit or half of the loss from holding ETH directly). The junior tranches would then receive the residual return on the asset, which would be even more volatile than

holding ETH itself. These can be thought of as a low beta and high beta versions of a crypto asset achieved through tranching. [28]

Asset Managers

Supply Aggregators

Yield farming involves investing in quantitative strategies that move capital across multiple protocols and platforms to generate the highest overall yield for the investor. Take Yearn Finance as an example. Anyone can create a vault on Yearn Finance, take in capital, and then begin investing it on behalf of others in a transparent, programmatic manner.[29] Some strategies may include lending, providing tokens to liquidity pools, and token farming.[30] These strategies can be layered on top of each other, sometimes making the vault strategies quite complicated. With Yearn, you always receive back the same kind of token that you initially invested.

As an example, say you deposit 100 ETH worth $1000/ETH in a yETH vault at Yearn. Assuming a collateralization ratio of 200%, the vault may then provide this ETH as collateral to Maker DAO to borrow $50,000 worth of DAI (this comes from [100*1000]/2). That DAI can then be deposited at a yDAI vault which in turn provides the DAI to a Curve yPool. Stable coins in the Curve yPool will be used to provide liquidity at Curve, thereby earning a portion of the trading fees generated by the AMM. The liquidity providers are also rewarded with CRV, the governance token for Curve, which fluctuates in price. The trading fees and the CRV tokens can be sold for ETH to provide a return to the initial investor. The investor would also keep their original ETH investment, which was initially provided as collateral. [31]

The strategies, platforms, and tokens involved can vary quite significantly across yield farmers, but the goal is always the same – maximizing total yield. For Yearn vaults, 5% of profits are set aside for gas fees. Of the remaining amount, the Vault creator keeps 10% and investors receive 90%. This means that investors keep ~85% of the total profits generated.

Traditional Managers

Other platforms allow you to invest in managers who oversee capital in a discretionary, semi-discretionary, or quantitative manner. For example, dHedge lists over 400 managers with some amount of capital, though most are quite small. [32] Zignaly allows your capital to be overseen by managers alongside their own capital, with payment through performance fees.

ETFs / Index funds

Collectively Organized

PieDAO uses a decentralized autonomous organization (DAO) to determine which crypto ETFs to create. Anyone who holds governance tokens is part of the DAO and can suggest ideas for new ETFs, which the community as a whole then votes on. Any given individual's voting influence is tied to the number of tokens that they hold. [33]

Currently, PieDAO offers a range of ETFs/indices including: DeFi Large Cap, DeFi Small Cap, BTC, ETH, and Metaverse NFT. The organization also offers some ETFs that combine these component indices. An interested investor typically supplies ETH to PieDAO, which then automatically converts it to the underlying components of the index. These purchases occur on a decentralized exchange, and the smart contract for the transactions is entirely collateralized. At the end, the investor receives a token specific to that index in return. When redeeming from an ETF, an investor can choose to receive back ETH or the various tokens underlying the index.[34]

Individually Customized

Set Protocol allows individuals to directly create customized indices of ERC-20 tokens that others can then invest in. Rather than having to convince a broader community to create an index like with PieDAO, this more unconstrained individual approach has led to over 400 "sets" being created. The underlying transaction dynamics are similar to PieDAO above, though Set offers a much greater diversity of indices. For example, there is even a FAANG Index that uses synthetic versions of the underlying stocks (supported by the Mirror Protocol) to create a crypto token that tracks the group's price movement. Some of the larger sets include the DeFi Pulse Index with $192mn and the ETH 2x Flexible Leverage Index with $110mn. [35]

A separate product that is not an ETF but is more customized to individual portfolios (rather than being broadly tradeable) is Barnbridge Balancer. It automatically rebalances a portfolio to a predetermined allocation (e.g., 60% BTC, 40% ETH). If one holding outpaces the others, the portfolio would be periodically rebalanced to maintain the target allocations. This way, no single position will grow too large as a percentage of your holdings.

Please note that for the "Markets" section of this paper I have chosen to focus on novel business models in DeFi, like automatic market makers. There are also many entities in DeFi that embrace a central order book model, similar to what you find in traditional finance. Apart from DeFi, there are also many centralized finance (CeFi) options that allow you to buy and sell crypto and crypto-related derivatives. These CeFi institutions are regulated and follow KYC and AML regulations.

Stablecoins & Macroeconomic Stability

Money and Its Creation

Money must: 1) be a store value; 2) a unit of account; and 3) a medium of exchange. [36] The initial money created by the central bank is known as monetary base (MB). MB can be cash or coin or it could be a commercial bank's reserves at the Fed (think about this as the deposits in a bank's account at the Fed). [37] MB is sometimes called narrow money. You can think of it as the first burst of money created. [38]

Commercial banks then expand the money supply through the credit creation process. This bank created money emerges through fractional reserve banking. Commercial banks are required to keep a fraction of their deposits at the bank (whether in their vault or at their account with the Fed). This fraction of deposits that must be kept in reserves is known as the reserve ratio. Anything more than this may be given out as bank loans or held in other safe assets (like U.S. Treasuries). [39] If a loan is given out, an individual or business receives that money and eventually spends it. Whoever is on the other side of that spending then receives the money and deposits it at another bank. If this happens over and over again, bank deposits end up being many times larger than the original increase in the MB. This graphic illustrates the process assuming an initial increase in the money supply of $1000 and a reserve ratio of 10%: [40]

Table 9.1: The Process of Credit Creation by the Banking System as a Whole

Required reserve (RR) (Rs.)	Deposit (Rs.)	Loan (Rs.)	Total reserves (Rs.)	Total deposits (Rs.)	Total loans (Rs.)
Initial deposit at U.B.I.	1000			1,000	
RR becomes 100		900	100		900
In second round (i.e. SBI)	900			1,900	
RR becomes 90		810	190		1,710
In third round (i.e., Bank of Borada	810			2,710	
RR becomes 81		729	271		2,439
In fourth round (i.e., Bank of India)	729			3,439	
RR becomes 72.9		656.1	343.9		3,095.1
Total			1,000	10,000	9,000

Fig. 9.2: How Bank Lending Creates Money

Deposits are considered money since, from the perspective of the deposit holder, this is money that can be directly spent on goods and services. The M2 money supply, sometimes known as broad money, includes: MB, checking accounts, traveler's checks, savings accounts, money market funds, certificates of deposit, and other time deposits. [41] This will hopefully provide some context when discussing the nature of stablecoins later on.

Attempts at Macroeconomic Stability

The Fed has a dual mandate of full employment and price stability. Its monetary policy is aimed at these two goals. If the Fed would like to boost economic activity, it expands the money supply through OMOs, which then leads to credit creation (see endnote 38). Specifically, the Fed targets the Fed Funds rate, which is the overnight lending rate among banks. OMO purchases of U.S. Treasuries create more USD reserves at banks, so that they then have an incentive to lend out these excess reserves to other banks which have credit worthy borrowers in their sights. Eventually, when individuals and businesses receive loans, they spend this money, which boosts GDP and employment. [42] However, expanding the money supply can also cause inflation, whether that is due to increased demand or to more money chasing the same number of goods.

If the Fed wants to tap the brakes on economic activity, it would sell U.S. Treasuries to banks, which reduces bank reserves, since the Fed receives cash for the sale. This reduction in bank reserves increases the interbank lending rate as the supply of interbank loans declines. This in turn affects the ability of banks to access capital and extend loans to individuals and consumers. Less credit availability means less spending, which reduces employment and inflation.

The Fed cares greatly about the narrow and broad money supply and the credit creation process, since these things are part and parcel with how it tries to achieve macroeconomic stability.

Attempts to Combat Systemic Risk

The credit creation process appears to be inherently unstable. Asset bubbles periodically emerge, credit is extended against these inflated assets, and purchases fueled by credit can push asset prices even higher. Bad credits especially get extended when those creating the credit have no skin in the game (e.g., if they immediately sell off loans to be securitized). When the asset bubble pops and defaults begin to occur, highly leveraged financial institutions see their equity wiped out.[43] This may make other banks hesitant to extend credit to the perceived struggling institution, which can precipitate insolvency. If a systemically important financial institution (SIFI) fails, there can be an immediate and enormous ripple effect, since such a SIFI is deeply enmeshed with the rest of the financial system. For example, derivatives exposure can often be 10x+ the value of the actual underlying assets. If a SIFI fails, then its counterparties on derivative transactions may now show heavy losses and naked exposure, whereas they previously believed themselves to be fully hedged. Uncertainty and fear pervade the financial

system as everyone tries to guess which financial institution will fail next, and credit pulls back from the entire system. A lack of access to capital, higher funding rates, and fear of a weak economy then lead banks to not extend credit to individuals and businesses, which reduces spending. The reduction in spending causes businesses to lay people off, which reduces incomes, which reduces spending. This becomes a self-reinforcing cycle.

The Fed will typically step in by flooding the system with liquidity, so that no further institutions become insolvent just by virtue of the pullback in liquidity. If an investment bank is on the brink of insolvency, the Fed will often try to broker its sale. If a commercial bank is insolvent, regulators will sequester its bad assets and push the remaining depositors and healthy assets to another bank. Congress may act to directly recapitalize the balance sheets of financial institutions, and the Fed may fund this through U.S. Treasury purchases with newly created money. [44] Fiscal stimulus helps offset the decline in consumption and investment (particularly when the Fed has hit the zero rate limit), helping neutralize the self-reinforcing cycles. Unemployment insurance can also act as an automatic stabilizer. To the extent that quantitative easing gets new dollars into the hands of consumers and businesses, this can be a source of additional spending as well. [45]

Concerns of the Fed & Regulators

The primary concerns of the Fed and regulators appear to be: 1) control of the money supply and the credit creation process to smooth macroeconomic outcomes; 2) prevention of and response to systemic risks; 3) protecting individual investors; 4) collecting capital gains taxes; and 5) fighting money laundering and terrorism. My sense is that is the rough order of their priorities. For the sake of brevity, I will not touch on #3-5, except to say that I think AML and terrorism concerns are a bit overstated. Privacy-focused layer 1 transaction protocols, like Monero and Zcash, are completely untraceable. It seems like any illegal activity would move through those channels rather than pushing its way through the DeFi stack (unless perhaps the stack becomes much more liquid than those privacy protocols).

There is now enough context to evaluate stablecoins.

Types of Stablecoins

<u>Fully USD Backed</u>

Stablecoins like USD Coin ($31.3bn) and Binance USD ($13.5bn) are fully backed 1:1 with U.S. dollars. This means that for each stablecoin created there is 1 U.S. dollar in a bank account. If you move out of the stablecoin, you would get that USD back and the stablecoin would be burned. Facebook's Diem will also be backed 1:1 with USD.

Partially USD Backed

Stablecoins like Tether ($68.6bn) and Dai ($6.5bn) are only partially backed by USD. Tether reportedly invests 30% of its reserves in commercial paper to generate some return, while the other 70% is kept in USD.

Dai was originally an attempt to create a decentralized stablecoin backed by cryptocurrency. Using a 200% collateralization ratio, one can deposit ETH and create 1 DAI, which is equal to 1 USD. If ETH falls in value, then you would need to deposit more ETH to maintain the collateralization ratio. However, this is an inefficient use of capital, since such a large amount of ETH would likely generate a higher returns elsewhere. Because of this, DAI was not able to attract enough ETH and opened up the types of collateral that can be deposited against it. This included other stablecoins, which have a collateralization ratio of only 101%. Over time, the collateral backing DAI has shifted towards stablecoins, which currently make up 61% of that collateral.

Not USD Backed

TerraUSD ($2.7bn) is not backed by USD at all. Instead, a related LUNA coin exists, and it is free floating. One must purchase $1 worth of LUNA coins and then convert them to TerraUSD (UST) to mint a new UST. Alternatively, if one wants to move away from UST, one would covert it to $1 worth LUNA and then sell that LUNA for USD. LUNA is speculative in that anyone can buy or sell the asset without an intention to convert it to UST. [46]

UXD is a newly emerging stablecoin that is also not backed by USD. To create a new UXD, one would deposit $1 worth of BTC. UXD's protocol then simultaneously shorts the same amount of BTC either through a perpetual swap or a BTC futures contract. This locks that $1 worth of value in, so that it always acts to back UXD. [47]

Vulnerabilities with Stablecoins

Tether (USDT) is reportedly 30% backed by commercial paper (CP). However, the individual CUSIPs for that CP are not made public. Also, no one has claimed to be a counterparty to these trades (Tether's CP holdings would be ~$20bn). It's possible that there is a completely innocuous reason for this. However, if there is any doubt about Tether's ability to stand behind its stablecoin, it could lead to a run on USDT. For example, say you believe that USDT is only 99% backed by USD or liquid equivalents due to losses on the CP. This might lead to redemptions out of USDT, since if everyone redeems, the last 1% of people would not receive their money back. As redemptions begin, they might accelerate as people try to avoid being in that last 1%. This could lead to a quick unwind of the stablecoin.

TerraUSD appears to have a structural vulnerability. If people begin to lose faith in TerraUSD, they can sell it and receive $1 worth of LUNA, which they can then sell for USD. However, selling the LUNA would cause its price to decline. Since LUNA's price has declined, the next person redeeming from TerraUSD would receive a greater number of LUNA coins (since $1 of LUNA backs TerraUSD and LUNA's price has gone down). They would then sell this larger number of LUNA coins to receive USD and so would push LUNA's price down even further. This could be a self-reinforcing cycle.

Likely Stablecoin & Regulatory Policy

If a stablecoin is backed 1:1 with USD, and the USD reserved against it is kept at a commercial bank account, then new MB is effectively being created. This is because the same amount of deposits remains in the system (they just transfer from the stablecoin purchaser's bank to the stablecoin issuer's bank) while a new form of money is created, namely the stablecoin itself. However, the Fed could instead require that these USD reserves be deposited directly at the Fed. This would keep the money supply the same, since total bank deposits would decline by the exact same amount that stablecoins increase by. This may affect the deposit funding of commercial banks, and it could impact more traditional credit creation. However, this should be offset to some degree by credit creation using the stablecoins. Requiring that stablecoin reserves be kept at the Fed would be a relatively easy way to maintain a stable money supply in the face of stablecoin issuance.

However, any non-USD backed or partially USD backed stablecoin is creating new money in way that would be much harder to neutralize. For example, consider UXD. Since BTC is a speculative asset, its price fluctuates based on marginal supply and demand for BTC. The Fed's expansion of the money supply may affect the price of BTC to some degree, but it is far from a one-for-one relationship. Many other factors affect the short-term movement and market cap of BTC. This means that a largely extraneous factor (the market cap of BTC) would impact how much UXD can be created. If UXD is equivalent to USD without being collateralized by USD, then it is the functional equivalent of new monetary base, and it is being created based on external factors (demand for UXD and the market cap of BTC) rather than at the discretion of the Fed. Since MB kickstarts the credit creation process that can affect consumption and investment, my sense is that Fed will be quite vigilant about putting an end to any stablecoins that are not backed 1:1 by USD. And for fully backed stablecoins, regulators will likely require that the reserves be deposited at the Fed.

The Fed will also focus on credit creation since that it how it typically attempts to smooth macroeconomic outcomes. My sense is that most lending against crypto right now is just used to buy more crypto. But if people start to purchase goods and services with their borrowings, then the Fed will pay greater attention. Also, if widespread payment rails evolve on stablecoins, then there will be regulatory focus on their robustness. Any potential for systemic risk (where that is defined as the ability to affect real world outcomes like consumption and investment at scale) will also be closely considered. Since non-crypto assets (like equities, commodities, real estate, etc.) are already regulated, their digital equivalents (created through

tokenization or synthetics) will also be scrutinized. Also, every financial instrument under "Markets" is regulated for other asset classes, so that will likely also be the case for crypto at some point.

My sense is that the Fed and regulators will require all stablecoins to be backed 1:1 with USD, specify particular digital wallets that can be used legally, and then attempt to create a permissioned system of regulated financial actors which can interact with these wallets. The first part of that (requiring all stablecoins to be backed 1:1) will happen in the near term, and the rest will probably play out over years. That said, it is not clear to me how regulation can be integrated into DeFi or whether the market participants would be open to that, even if it were possible. [48] VPNs will continue to be used to engage with DeFi as it currently stands, regardless of legality, so there may be limits to what the Fed and regulators can do.

A remarkable and beautiful DeFi ecosystem has blossomed over the past couple of years, and my hope is that regulation walks the right tightrope without either killing off the continuing rapid innovation or pushing it abroad.

Facebook's Diem: The Dollarization of Developing Economies

So far, we've been looking at intersection of stablecoins and macroeconomics from the point of view of the U.S. However, now consider a developing economy with a less established fiat currency. When Facebook's Diem is launched, it seems like citizens of developing countries would likely prefer the stability of a USD equivalent to their domestic currency. They would likely try to hold their savings in Diem. Similarly, businesses in those countries would likely prefer to receive the USD based stablecoin as well. If this happens at scale, then there would be an effective dollarization of developing economies. Domestic central banks would now be changing the supply of a currency that few people use, so they would lose the ability to impact macroeconomic outcomes.

Given this possibility, my sense is that most developing countries will not allow Diem to be used as legal tender as it is currently constructed. Instead, Facebook will likely have to create many different versions of Diem, each of which are linked to and backed by a particular currency. A country-specific version of Diem could then be used for transactions in that country.

Central Bank Digital Currencies

A central bank digital currency (CBDC) is operated directly by a central bank (at least in terms of maintaining a single ledger of transactions on the back end) and represents a legal claim against the central bank. This contrasts with the money currently in your checking account, which exists in a ledger at a commercial bank and is a claim against that bank (even if the account is ultimately insured by the FDIC).

If the Fed introduces a CBDC, it would very likely involve intermediaries like payment processors, since it would otherwise have to directly assess and negotiate issues like fraud. However, even if it outsources this function to payment processors, the very existence of a CBDC would likely open up the Fed to criticism related to distasteful actors engaging in perfectly legal transactions. It might also face more justified criticism for ultimately allowing transactions tied to genuine crimes. Foisting responsibility onto the payment processors can only go so far if the CBDC is seen as ultimately belonging to the Fed.

There are also substantial privacy concerns. Currently, many different centralized ledgers exist at the various commercial banks, but no one entity has immediate transparency into all of these ledgers. [49] However, a CBDC would tend in that direction, depending on whether it is designed as a supplement to the current system or a replacement of it. While technological and governance structures would supposedly prevent abuse of this power, my sense is that the average citizen may not fully trust such safeguards. [50] On the positive side, a CBDC would reduce the network effects of particular payment processors and so reduce their fees. This reduction in fees would also enable micropayments. [51]

Another argument for CBDCs is that they allow for explicitly negative interest rates. For example, if you want to spur demand, you could outlaw physical money and then begin to burn the money in people's digital wallets, providing them with an incentive to immediately purchase goods and services before their money disappears. Currently, we have negative real interest rates since the inflation rate is higher than the deposit rate. However, if our currency were to be manipulated so directly, I suspect that there could be an overwhelming loss of faith in it. Instead of purchasing consumer goods and services, people would likely begin to move into a digital asset like BTC, which has a limited supply and is hard to confiscate.

Appendix: Virtual Worlds

The development of virtual reality and the natural human interest in games could lead to a blossoming of virtual worlds in which people interact in extraordinarily complicated ways. Financial linkages back to the real world could even allow some people to spend most of their time in a virtual world. [52]

Political Governance

Since these virtual worlds will involve groups of people interacting with each other, they will be inherently political. Some form of political governance will exist. Perhaps people will start in a state of nature, and we might see what emerges. Perhaps the first X number of people to join will find themselves in a constitutional convention where they get to decide how to structure their political life and what the decision-making rules will be going forward. Perhaps the virtual world's creator will pre-determine that constitution along with ways to amend it. Perhaps there will be a direct democracy without any kind of further institutional constraints. All of the typical political issues (federalism vs. centralization, a separation of powers, etc.) would also come into play. There could also be substantial variation in voting methods (first-past-the-post, approval voting, IRV, etc.) as well different weightings given to votes (based on time spent in the virtual world, skin-in-the game via ownership of digital assets, etc.).

Economic Governance

Similarly, the economic rules of the road could differ enormously across virtual worlds. Perhaps some virtual worlds will find an effective alternative to market prices (even if every attempt in the real world has failed miserably). Some worlds may have no safety nets, while others may evenly redistribute half of all income each year or have a hefty universal basic income (or an EITC to help only those who are working in the virtual world). Some worlds might fund this redistribution through fiscal policy, while others explicitly create new money each year to fund a UBI. Some setups could have only an official currency while others have only private currencies. Another possibility is a mix of the two. Some economies could be tightly regulated while others are more laissez-faire. The possibilities are endless.

Choice and Competition

Choice and competition have spurred improvements in every good and service in our economy. Given how low the switching costs are between virtual worlds, the creators of those worlds would be strongly incentivized to maximize the welfare of the average participant. People would flock to the worlds where they feel like they are sustainably thriving. Part of the reason that this interests me is that if new and effective models of political and economic governance are discovered, they could potentially be pulled back into the real world. We would certainly need to be cautious that some part of our current world has been underspecified in the virtual world. However, such an explosion of virtual experimentation may end up being a great boon.

Endnotes

[1]This is a simplified version of the stack in "The DeFi Stack" by MultiCoin. Their article is a very pithy but still comprehensive look at DeFi, and I'd highly recommend reading it.

[2] Additionally, cTokens, aTokens, and the liquidity provider shares of aggregated market making pools can be used as units of value. I didn't want to mention these things in the body of the paper at this point since they may be unfamiliar to some, and the paper will go through them in more detail later on.

[3] You can find much more detail about the emerging Layer 2 solutions on Ethereum in "In Search of Scaling: A Guide to Layer 2" by Galaxy Digital Research.

[4] You can track the DEX volumes at CoinGecko.

[5] "The Separation of Time and State" by MultiCoin provides a sense of proof of history, while "What is SOL?" by Whiteboard Crypto might be more digestible.

[6] ERC-20 tokens are designed and used solely on the Ethereum blockchain.

[7] Aave is a competitor to Compound with basically the same business model. The tokens that it issues on its deposits are aTokens. aTokens were mentioned in a previous footnote.

[8] In the example of DAI, the utilization rate (U) would be: U = (amount of DAI borrowed) / (total amount of DAI deposited). An example of a borrowing rate might be: (borrow rate) = 2.5% + U * 20%. An example of the deposit rate might be: (deposit rate) = U * (borrow rate). There's not really any "profit" on the spread between the deposit rate and the borrowing rate, since there are typically more depositors than borrowers. This means that the apparent spread mostly goes to making sure that all of the depositors receive their interest.

[9] The Compound whitepaper is a good resource and "Lending and Borrowing in DeFi" by Finematics uses video animation to explain the dynamics behind Compound and Aave.

[10] The lending and borrowing rates for various assets on Compound are directly listed on its webpage.

[11] Aave is a competitor to Compound with a similar business model. The tokens that it issues on its deposits are aTokens. aTokens were mentioned in a previous footnote. Deposits and lending across all of the top platforms can be seen here.

[12] This is from: ([(10/9.8)^2] – 1) * 100% = 4.1%. The fixed rates offered will vary day-to-day depending on the value of epETH, but at the point in time that you purchase epETH, you will receive the associated fixed rate if you hold the asset to maturity.

[13] The Element whitepaper is very clearly written and goes into more detail. "Element Finance for Dummies" by defi bae may also help some.

[14] Aave offers fixed borrowing rates, but such rates are typically a good bit higher than the related variable borrowing rates. If variable rates are the more rational pricing mechanism, then the higher fixed rates may be meant to provide a buffer against circumstances that would otherwise have led to an increase in the variable borrowing rate.

Aave also offers flash loans which are worth millions of dollars and don't require any collateral. However, such flash loans must be repaid on the same Ethereum block (i.e., within ~13 seconds), so that there's no risk to the loan from Aave's perspective. Flash loans are taken out by arbitrageurs who may attempt to buy a cryptocurrency at a slightly lower price on one exchange and then immediately sell it at a slightly higher price on another exchange.

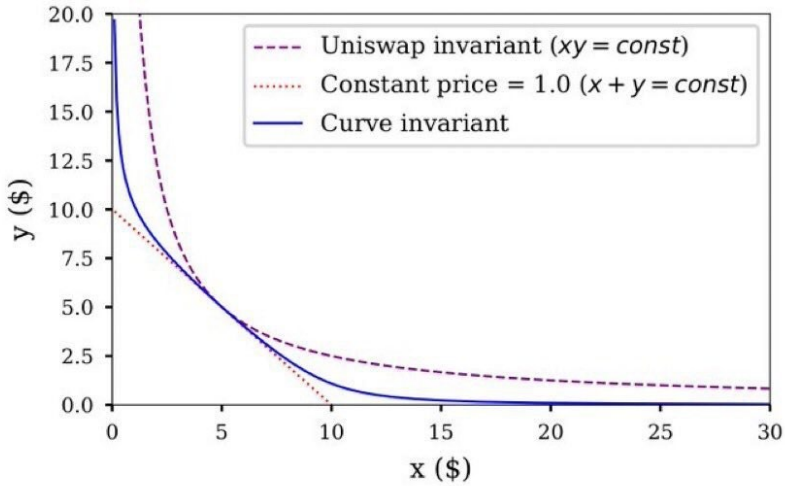
[15] If you are more of a visual learner, then several videos have been created that provide a sense of how AMMs work. Some good ones include "What is Uniswap – A Beginner's Guide" by 99Bitcoins; "What is an Automated Market Maker" by Whiteboard Crypto; and "How do Liquidity Pools work?" by Finematics.

[16] This comes from "Uniswap and the AMM Model" by Giorgio Giuliani on FinTech Ruminations. Interestingly, anyone can create an ERC-20 token (e.g., on Roll), provide the token and another asset to a Uniswap liquidity pool, and then enable public trading of the token on Uniswap.

[17] While it is beyond the scope of this paper, it is worth noting that liquidity providers (LPs) face the risk of impermanent loss. Impermanent loss is the loss suffered by providing liquidity to an AMM when this situation is compared to the scenario in which you had just held the two assets (of the same total dollar amount) without introducing them to the pool. "What is Impermanent Loss in Crypto?" by Whiteboard Crypto provides a quite clear explanation of impermanent loss. Impermanent loss increases as an exchange rate moves to extremes. In response to this, Uniswap v3 introduced the idea of concentrated liquidity, where LPs only provide liquidity within certain ranges around the current price. This can boost returns for the LP, sometimes quite substantially.

[18] Stablecoin pairs (like USDC/DAI or USDT/USDC) should be tightly correlated, since they are all pegged to the dollar. There are also ERC-20 tokens that have been minted which represent BTC, so that an equivalent of BTC can be traded on the Ethereum blockchain. These include wBTC, renBTC, and sBTC, among others. These tokens should also trade together. Curve Finance uses a unique algorithm to straighten the middle portion of the exchange rate curve, so that these exchange rates (which are the slope of the lines below) stay relatively constant

across a greater range of trades. The DefiWeekly substack by Kerman Kohli has a graph which illustrates this:



[19] The trading volumes of the various decentralized exchanges can be seen here.

[20] Stablecoins that Mirror accepts include: TerraUSD (UST) and aUST. Other assets accepted as collateral include: mAssets, Terra (LUNA), bLUNA, MIR, and ANC. Terra is the free floating token which is used to keep TerraUSD stable (more on that later). bLUNA is bonded LUNA that is backed by underlying LUNA tokens (these LUNA tokens act as collateral for loans taken out on the Anchor Protocol). MIR is the governance token for the Mirror protocol. ANC is the governance token for the Anchor Protocol.

[21] Counterintuitively, when you mint a mAsset, you are actually short that mAsset, even though you now own it. This is because you are obligated to return that mAsset to the Mirror Protocol in the future to free up your collateral. If the mAsset price goes up, you do not benefit since the mAsset will be returned eventually. The only way that a minter can make money on an mAsset price change is if the minter immediately sells the mAsset after minting it, the price of mAsset falls, and then the minter purchases it and returns it to the protocol to free up the collateral. However, if you own a mAsset, you can always generate a return on it by being a liquidity provider.

[22] I'm focusing on European options here since that is what Opyn, the company that I will mention later, trades. Most non-crypto options are American options, which can be exercised at any point before expiry (and not just on the expiration date itself, like with European options).

[23] In traditional finance, much less capital is needed to write options since all of the relevant exposures are continuously hedged. For example, if you write a call option on a stock, you could short the underlying stock to delta hedge it (where the "delta" is the option's sensitivity

to the price of the underlying stock). You could also hedge the option's exposure to interest rates, volatility, etc. This would have to be done on an ongoing basis, since each sensitivity will likely change over time.

[24] Opyn seems like a cleverly designed system. That said, it seems like one point of vulnerability could be if the spot shock is too conservative, leading to not enough margin being initially set aside. Also, if required margin levels are breached en masse, the liquidation process could get a little disorderly.

[25] The size of the funding payment is: (notional position size) * (funding rate). And the funding rate is: (TWAP on Perpetual – TWAP of Market Index via Oracle)/24. TWAP stands for trade weighted average price. Prices for both Perpetual and the Market Index get recorded hourly for each of the past 24 hours, and the more recent hours are weighted more heavily. Dividing by 24 normalizes the number to a single point in time. If the funding rate is positive, then the Perpetual price is too high relative to the spot price, and the funding payments go from longs to shorts. If the funding rate is negative, then the Perpetual price is too low relative to the spot price, and the funding payments go from shorts to longs.

[26] I would highly recommend reading everything under "How It Works" in the Perpetual explanatory documents. The reasoning behind their setup is very clearly explained with quite helpful examples.

Separately, this is a great site that keeps track of some key metrics on the Perpetual protocol.

[27] These graphics are taken from the Barnbridge whitepaper, which is very clearly written.

[28] I don't know why they use "alpha" in the name, since this is just a low and high beta version of the underlying crypto asset.

[29] Since everything is executed through smart contracts on the blockchain, the individual holdings and strategies can be seen transparently.

[30] Token farming is when you provide capital to a lending platform or AMM with the aim of receiving the related governance token (in addition to an interest rate or trading fees). Governance tokens trade publicly, and their price can fluctuate substantially. They can be quite a draw, since an investor could make a net profit on these tokens, even if the associated activity is losing money (e.g., if the LPs to AMMs are experiencing impermanent loss).

[31] "What are Yearn Vaults?" by Finematics provides an illustrated explanation of yield farming.

[32] You can see the managers on dHedge's website. Even the largest managers are quite small by traditional finance standards. The only reason that I have called them "traditional" managers is that they are using strategies that might be more familiar compared to things like yield farming.

[33] DAOs allow for the decentralized, cooperative governance of a community. They stand in contrast to centralized forms of organization and governance. DAOs are voluntary, unlike governments, and they are decentralized, unlike corporations. This makes it more likely that any value generated will accrue to its members.

[34] Given that Pie's fees are only 0.7%, it doesn't seem to make sense to pay the 2-2.5% management fee of a BitWise or Grey Trust, unless you're a large institution that needs to be regulatorily compliant in very specific ways.

[35] You can explore the available indexes on Set's webpage.

[36] While I know that you can purchase things in crypto, my sense is that the store of value function is necessary to function more broadly as money. If you think crypto is going to rise in value, you may be hesitant to part with it to purchase a good or service. On the other hand, a business may not want to accept crypto if its value can drop substantially before the business begins paying its costs.

"Unit of account" means that you can price things in the currency. While goods priced in crypto can have constantly adjusting prices based on how crypto is fluctuating, it's worth noting that this can happen only because USD exists and the USD price of the good is constant. The crypto price then fluctuates relative to that constant USD price.

[37] From now on, most of my examples are going to be U.S. based for the sake of simplicity.

[38] The Fed increases the MB through open market operations (OMOs) in which it purchases U.S. Treasuries from banks and gives them new money in return. Since the banks have deposit accounts at the Fed, this just involves increasing the numbers in those accounts. On the other hand, if the Fed wants to reduce the money supply, it sells U.S. Treasuries to banks and receives money from them (this reduces the money supply). Banks are required to participate in these OMOs.

[39] This means that, on its own, a bank could not cash out any meaningful portion of its depositors, since the money has been lent out to others. This led to bank runs before the FDIC was created, since even the perception of insolvency led depositors to rush to the bank to get their money back, while there was still some there. This in turn could cause a solvent bank to become insolvent. The FDIC now charges banks an insurance fee and guarantees that depositors will receive the full amount of their savings back up to $250,000 per bank. This way, individuals do not have an incentive to rush to the bank at the same time to pull out their deposits.

[40] This graphic comes from here, though you can find a similar chart in any introductory macroeconomics textbook. Given a particular reserve ratio (RR), the maximum amount of deposits that be created is: (initial increase in money supply) * (1/RR). In the example, this is

$1000 * (1/0.1) = $10,000. In reality, the amount of deposits created may be less than this, if people hold into physical cash or banks choose not to loan out all of their available reserves (e.g., if they can't find credit worthy borrowers or if they think that their balance sheet might be impaired).

[41] As odd as this sounds, money exists on a spectrum from immediately capable of being spent (like coin and cash and checking deposits) to liquid on short notice (savings deposits, time deposits, etc.). The more liquid and immediately capable of being spent something is, then the more like money it is. There are different definitions of money ranging from MB to M4, depending on what you include in it.

[42] It's an open question whether this is always a good idea. GDP is the sum of the incomes in a country. If debt/GDP grows too greatly, then individuals and businesses may not have enough income to service those debts. In that case, the debts will either need to be restructured, defaulted on, or inflated away (or some combination of those things). If a government does not control its own money supply (e.g., countries in the EU or countries with USD pegs), then the government faces the possibility of default as well, since it can't just print more money to pay its lenders.

If you'd like to learn more about macroeconomics in general, Bridgewater is a great resource. Their framework for economic analysis of "How the Economic Machine Works" is laid out in a larger piece, a more digestible piece, and a video.

Lyn Alden is also a great source of macro analysis, including in relation to cryptocurrencies.

[43] Assets are everything that a business owns that has value. Liabilities are all of the things that a business owes others. For an individual, your total assets minus your total liabilities would be your individual net worth. For a business, assets minus liabilities is shareholder's equity. It's the net worth of the business that shareholders have a claim to.

Now, let's take the example of a commercial bank. Say its initial investors put in $1mn (through common stock), and it has accumulated profits over the years of $1mn (retained earnings). This means that total shareholder's equity is $2mn. Now, say that bank has taken in deposits of $98mn. These deposits are liabilities since the bank owes those deposits to other people. That money belongs to the depositors – not to the bank. The depositors are essentially loaning money to the bank and are being given a small interest rate in return. The bank then takes that money and loans it out to individuals and businesses at a higher interest rate. The bank makes a profit on the spread between these two interest rates. It has $100mn to loan out (the $2mn + $98mn) and let's say that it loans out the full amount in bank loans. These bank loans are assets for the bank, since it owns those loans and they have a economic value tied to their future repayment. However, the bank is now very levered since its assets/equity ratio is 50x (from $100mn/$2mn). If the bank experiences defaults and has to write down its loans by even 2%, then its entire equity has been wiped out.

[44] I'm not saying that this is fair or that all of it is necessarily good in every respect. I'm only saying that this is how things appear to play out.

[45] This is happening with QE3 during the pandemic, as Congress is sustaining heavy fiscal stimulus and the Fed is funding these actions through bond purchases with new money. The new money is going directly into the hands of potential consumers.

[46] I have focused on the 5 largest stablecoins so far, but a full listing can be found on CoinMarketCap, and this site and The Block are also good sources of data.

[47] For example, say you deposit $1 of BTC and the protocol goes short a perpetual swap on the same notional amount of BTC. If BTC's price rises, then the deposited BTC would increase in value. However, the short BTC swap's value should decline by the exact same amount. This locks in the $1 of initial value. The process would occur in reverse if BTC's price were to fall after its initial deposit.

[48] That said, at least one permissioned decentralized exchange does exist.

[49] China is currently leading the way with CBDCs, but that's because it is happy to oversee every single transaction in the country and potentially block transactions or empty digital wallets at its own discretion (e.g., with political dissidents).

[50] Nathaniel Whittemore has an excellent podcast called "The Breakdown with NLW" at Coindesk. It deals with the intersection of crypto and macro/policy. This episode and this episode had an impact on my thinking. The second episodes mentions "Are Central Bankers Ready for Payments Theater?" by JP Koning.

[51] The Royal Bank of New Zealand recently put out a paper called "The Future of Money – Central Bank Digital Currency" which very clearly describes and illustrates the key issues.

[52] I'm not saying that this would be a healthy thing to do – only that it might be economically viable given play to earn models.