DeFi: The Financial Fabric of the Metaverse

Decentralized Finance, known colloquially in the cryptocurrency community as "DeFi," has been promoted as a form of finance that will replace traditional finance, or "TradFi" as described by the same community. The purpose of this paper is to look through the various claims to understand the technology and financial processes that underpin the DeFi phenomenon and separate the hyperbole from the true innovations so the reader can see what may be enduring and worth a professional's time to understand. The paper concludes that while there are important ideas starting to emerge from the DeFi phenomenon, there is also a lot of risk and very little that a prudent investor would consider as opportunities worth pursuing at this time. DeFi is the financial system of the metaverse, and while that's innovative, it is not a replacement of, nor an asset in, the traditional financial system.

Peter Horne
has worked for over 30 years in product and technology development in the financial services industry, and has worked in Australia, the USA, and Hong Kong. Peter maintains an active interest in developing cybersecurity and cryptocurrency systems, and was credited by the New York Times for discovering the Superfish Spyware (https://bits.blogs.nytimes.com/2015/02/19/researcher-discovers-superfish-spyware-installed-on-lenovo-pcs). Peter is also a Research and Development Associate at Northfield Information Systems, and holds a B.Sc. (Hons) from the University of New South Wales.

PROLOGUE

It makes one wonder where one's career went wrong when you are looking at a decentralized financial (DeFi) exchange called "Sushi" that proclaims; "Michelin star-worthy DeFi innovations crafted by our master chefs" who "cook up the tastiest dishes in DeFi." Absurd, except that the Sushi DeFi protocols have $1.95B of notional value locked into its liquidity pools, and it has had $168B of total turnover. To put that into perspective, the total U.S. sushi restaurant market size in 2021 was $27.5B.[1] And of that $168BN of Sush DeFi turnover, some of it went into "CrypToadz by GREMPLIN"; a collection of non-fungible tokens (NFTs) that point to computer generated pictures of toads. Those toad pictures have had over $190M of turnover on the OpenSea marketplace[2], and that will only be a portion of the trades as many will also occur person to person via blockchain transactions. Yet while these numbers make a banker's eyes water more than a raw wasabi root, Sushi DeFi is a pantomime of financial themes on top of childish memes. It is absurd when viewed through the prism of traditional finance (called TradFi by those in DeFi) where regulated intermediaries serve real business activities in real economies.

In my last paper, I made the case that cryptocurrencies were being integrated into the regulations and institutions of the traditional financial system and that this process was good for investors because it will make these assets more trustworthy and better understood, and the processes should also test their utility and longevity. In this article we are writing about DeFi concepts, which are built on top of cryptocurrencies which means that we are in effect observing the second moment of cryptocurrencies without determining if the first moment is useful and here to stay. So if its manifestations are absurd and we don't know if it's built on something made to last, why bother writing this paper? The reason is that I believe that underneath the craziness of DeFi projects are new technologies and practices emerging that are important to understand, and some innovations may even live beyond the cryptocurrencies that gave rise to them. I did the work to look at the toads, the bored apes with their yacht clubs, the endless whitepapers pronouncing revolutions in finance and social funding, the declarations of the death of TradFi and exchanges, and the "millenial gold" hyperbole. But through that process what I have found and hope to present in this paper is an analysis of the fundamental innovations going on, albeit in strange ways, that I believe are worth a professional's time to understand because the innovation of the blockchain has only just begun.

INTRODUCTION

In a world of endless competing narratives and terminology, web3 (stylized as all lower case as a nod to

its programmer origins) has to stand out as one of the most confused terms in the cryptocurrency sphere. On any day, my Twitter feed suggests to me that web3 is anything from a technology through to a taxonomy, spilling over into a millennial social movement. The genesis of web3 is that it is a technology term; the name given by the original Ethereum developers to the application programmer interface that allows a user program to talk to an Ethereum network node to perform transactions and execute smart contracts. It was called web3 to proclaim a new decentralized internet that is enabled by blockchain technology and end user cryptocurrency transactions, and to distinguish it from the centralized, corporatized Web2.0 model where all our logins are controlled by Google, Apple and Facebook. As it grew in profile it came to describe the category of projects that used it, like "social media" described new media projects. Then, given the predominance of use cases, it became totemic among tribes of advocates, especially in artistic communities and those experimenting with the idea of decentralized autonomous organizations (DAOs). Recently, I have seen it used to cover anything to do with cryptocurrencies, including Bitcoin. And so given everything is web3, the terminology I use for this paper is:

- Cryptocurrencies - blockchain protocol currency systems such as Ethereum and Bitcoin that rely on a decentralized transaction verification process.

- web3 - the overarching category of technological, cultural, corporate, and work practice innovations that are enabled by cryptocurrencies and programmable blockchains.

- Programmable Blockchains - Cryptocurrencies that support smart contracts with a focus on the Ethereum blockchain.

- DeFi - smart contract managed finance activities related to the creation, buying and selling of smart contract defined and managed tokens. This includes DAO tokens which represent organizational activities and provide other methods to control other smart contracts.

- Digital Currencies - blockchain protocol fiat currencies such as central bank digital currencies.

I have addressed the rise of cryptocurrencies in my previous paper, "Integrated Crypto: And why that's good for Investors," and I have dealt with web3 as a generally accepted catch-all description of the phenomenon that is arising from the integration of cryptocurrencies into technology, finance, and culture. In this paper, I will take the reader on the next leg of the journey through my analysis of programmable blockchains, DAOs, and DeFi, and then look at how all of these are starting to be a significant influence in the real worlds of finance, technology and society.

PROGRAMMABLE BLOCKCHAINS

The fundamental innovation of the blockchain invented by the illusive Satoshi Nakamato[3] is that it enables a peer-to-peer network of adversaries to trust a shared history of messages. Bitcoin was the first blockchain, and its messages create a ledger of transactions performed between users of the Bitcoin cryptocurrency. However, blockchain message content can be anything the network agrees is a valid message, including program installation and program execution messages, and the title of the first truly programmable blockchain goes to Ethereum. Note that I said "truly programmable," because it is true that the Bitcoin blockchain also implements transactions as messages that contain simple instructions similar to the Forth programming language. Theoretically, Bitcoin could be allowed to process user installed programs, however the bitcoin core developers that control the code base have never allowed this to occur for reasons that range from the scale risks of adding additional transaction types, through to Bitcoin shibboleths about blockchains only being useful for value transfer transactions. It was this intransigence that caused Vitalik Buterin to start the Ethereum project, and the goal from inception was to create a blockchain that was Turing Complete; a self referential definition meaning that a Turing Complete computer can can implement a Turing Machine to pass the Turing Test, which in lay terms means that it has all the operational codes to write completely functional programs. The Ethereum developers called these programs "smart contracts."

THE UNIVERSAL COMPUTER

The Ethereum blockchain contains both financial transaction messages for mining and sending the

Ethereum (ETH) cryptocurrency to and from network addresses (wallets), and for sending data messages to and from wallets. If a data message is sent to the network that is an encoded program that can be loaded by the Ethereum Virtual Machine (EVM), then the Ethereum nodes will construct the program at the node using the program code in the message. In simple terms, this is the process to create a smart contract. If the data message is encoded as a function call on a smart contract, then the node will call the smart contract with the function parameters. The effect of the node executing the smart contract code with function call data is that the EVM performs functions that imply the storage and retrieval of data, and the performance of other user designed functions on the data. By rolling the blockchain forward from the genesis of the blockchain, and recording the effects of the data instructions in the EVM on local node storage, all nodes adhering to the blockchain rules can in effect get to the same shared state. To use a personal computer (PC) analogy, the Ethereum network allows each participant to unbox and construct a PC with the same central processing unit (CPU), standard disk drive and network connection, and by receiving blockchain messages and executing the same CPU chip instructions in correct order, a database is constructed on the PC that is a perfect copy of the database held on all the other other PCs processing the same instructions. Once this process is complete, any query you make on your PC on your node will return the exact same data and calculation output as what would be seen if you had performed the task at a different PC that had performed the same process. The effect of this process is to create what can be called a "universal computer."

An important concept to understand with the Ethereum network is the "gas" charging mechanism that regulates the cost of installing and calling smart contracts on the network. The "universal computer" may be universally accessible, but its resources are not anywhere near universal size. To extend the PC analogy, the EVM is like a 1984 PC that provides acceptable performance for the retrieval of information by calling data-read smart contracts at each node, because each node has a copy of the data. But when it comes to installing programs and storing data which are data-write operations, it is as if everyone is using only ONE universally shared 1984 PC. To manage this shared resource, the cost of installing and running smart contracts that write data is charged in units of "gas," paid for in Ethereum. In simple terms, gas units are arbitrary weights assigned to EVM instruction codes and data storage block sizes, and so the total gas cost depends on how large and how complex your program is to install and run. Before you submit a transaction, the node will do a dry run of your request and estimate the gas usage, and then it's up to you to set the price in Ethereum that you are willing to pay per unit of gas. The gas of all transactions in a block is paid to the miner who wins the competition to mine the block onto the blockchain, and the gas price at any point in time is set by a competition among miners competing to fill blocks, which means that the cost of gas varies according to network usage. This means that the more people compete to use the blockchain, the higher the cost of gas, which also means that the use cases and participation of the Ethereum network are also limited. A better description of the Ethereum Universal Computer is perhaps that it's a universally accessible timeshare computer that can only support a very small planet of the people that can afford to use it.

COMPUTERS NEED AN OPERATING SYSTEM

If we look back to our PC of 1984, we see the days of CPM, MS-DOS, Apple DOS, VMS, and System/360. These were all different operating systems that had different ways of loading programs, writing programs, and sharing data between programs. The EVM is a virtual machine and there are many ways it could be driven, but the Ethereum ecosystem settled on the Solidity program language as the standard way to implement smart contracts on the EVM. Just as Microsoft created an operating system that made an application programmer interface (API - originally defined in the C programming language) that made shared windows components available for use by developers to move business processes to the PC, the Ethereum ecosystem created the Ethereum Request for Comment (ERC) standard as part of the Ethereum Improvement Process (EIP) to formalize the standards and conventions for application level components such as smart contracts, names, etc. that use the Solidity language on the Ethereum blockchain. With the Ethereum Foundation acting as the Microsoft of the blockchain world, they have created a code sharing and program interoperability dynamic which is akin to creating a shared operating system for smart contracts. Programmers can use the operating system to share data

models, perform transactions, and service providers can integrate with them and compete on user engagement and experience.

IDENTITY AND PAYMENTS

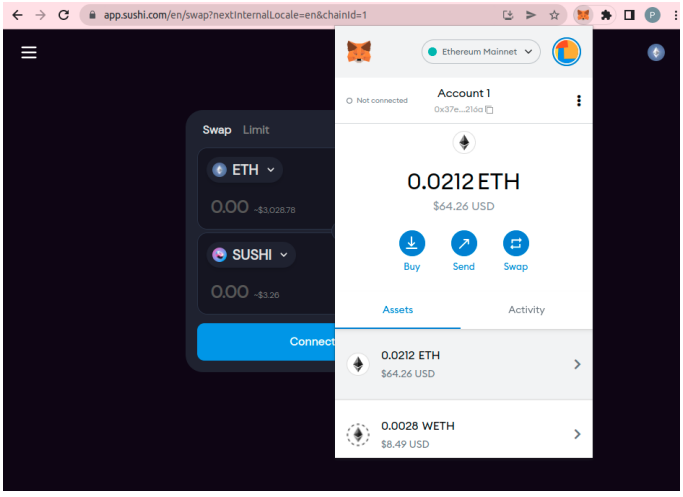
The reason why Web2.0, with all its centralized social platform login tools, is so ubiquitous is because it has made user identity and access to services integrated and simple across multiple web applications. Likewise, Web2.0 payment systems where identities are also associated with accounts that are integrated with credit cards and Paypal has meant that users have quick access to payment systems in order to perform transactions at the point of service. In the web3 world, these services are provided by the crypto wallet application, most commonly added to a user's web browser as a secure plugin.

Wallet applications are quite the wonder of the web3 world, and Figure 1 shows the popular Metamask wallet plugin ready to perform a transaction on sushi.com. After installing the plugin, the user can either create a new crypto wallet (which in simple terms means generating a new random cryptocurrency private key) or re-enter an existing wallet by entering backup data known as "wallet words." The user can then fund the new wallet by either sending some funds to the wallet address on the blockchain from a fiat crypto exchange where they bought their crypto for cash, or if it's an existing wallet, the wallet application can connect to any web3 node and find out the user's balances from the blockchain. Once set up, any web application can ask the user to cryptographically sign data using their wallet application enabling the web application to perform transactions, and it can also be used to identify users as being the owner of an account. Et voila, we now have a decentralized identity management system with an integrated crypto payment system that is completely under the users control and with no intermediaries as all information is shared through the blockchain history that is available to everyone. If applications add the public data from blockchain identification services such as The Ethereum Name Service (ENS) where people voluntarily create names and add other information, the wallet system also becomes a distributed reputation system.

DEFI STANDARDS

And so the universal computer with its operating system and access control and payment systems are now ready for something to do, and in the spirit of cryptocurrency developers rethinking the money system, the Ethereum user community set off to rethink all aspects of the financial system. No one asked them to, and many people don't want them to, but just as the PC was a disruptor in the era of the centralized mainframe, the decentralized universal computer, its operating system and emergent standards body, are here to disrupt centralized financial systems. The sheer weight of cryptocurrency capital available to the hands of

Figure 1: Metamask Wallet on sushi.com web application



unorthodox investors to spend on projects that range from the simple to the complex (or the trivial to the serious) all means that the ecosystem just keeps growing unhindered, and now it has its own category in the world finance - DeFi.

To understand DeFi we first have to understand the shared components created by the ERC process and how they enable financial transactions. There are many ERC managed proposals, but the two key ones are the ERC20 standard for defining and managing ownership of fungible tokens, and the ERC721 standard for defining and managing ownership of non fungible tokens.

ERC20

The ERC20 standard[4] defines the methods a smart contract must implement to create and manage the ownership of fungible units known as "Tokens" that are deemed to be of the same type by virtue of them being under the management of the same smart contract. In TradFi equivalents, an ERC20 smart contract is the source of truth share register of all shares issued in an entity, combined with the custody bank processes of transferring ownership from one shareholder to another. As smart contracts have unique addresses represented by cryptographic hashes stored on the blockchain, I define an ERC20 token as being the units of a specific ERC20 contract hash.

A good example of an ERC20 token is the USDC stablecoin. The concept of the stablecoin is to use the cryptocurrency "payment rails" as they are called for decentralized transactions, but not have the volatility of cryptocurrencies when used in trade. The most popular stablecoins are those that track the USD as that is the most popular fiat currency in trade. That fact is loaded with irony given that cryptocurrencies were designed to replace fiat currencies, however, it points to the evidence that the payment rails established by cryptocurrencies are a valuable innovation in their own right.

The USDC stablecoin is regulated and holds approved USD assets in a trust, and then for every USD held in the trust account, the units of the smart contract at address

0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48[5]

are "minted" (created) or "burned" (destroyed) by the administrator according to inflows and outflows in the trust. Because this is an ERC20 compliant smart contract, Figure 2 shows how anyone can look at blockchain tools such as etherscan.io to see the information about the token. Likewise, exchanges or individuals can buy or sell their holdings in this contract either at an exchange, or privately as a party to party blockchain transaction.

Note that it is unusual for tokens to be asset backed by assets in the real world; most represent value for assets created "on-chain," which have a purpose defined by the developer, and have a value because someone says it's valuable. Most ERC20 tokens are using the Ethereum cryptocurrency blockchain to create a smart contract that, in effect, defines another cryptocurrency.

Figure 2: etherscan.io USDC ERC20 Token Query

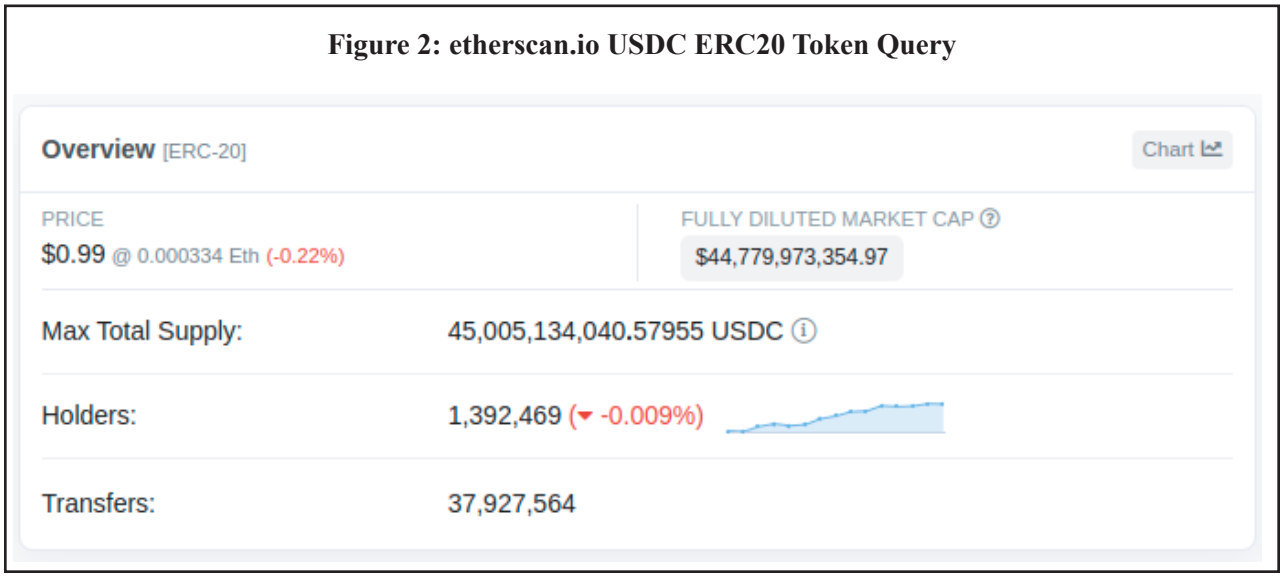
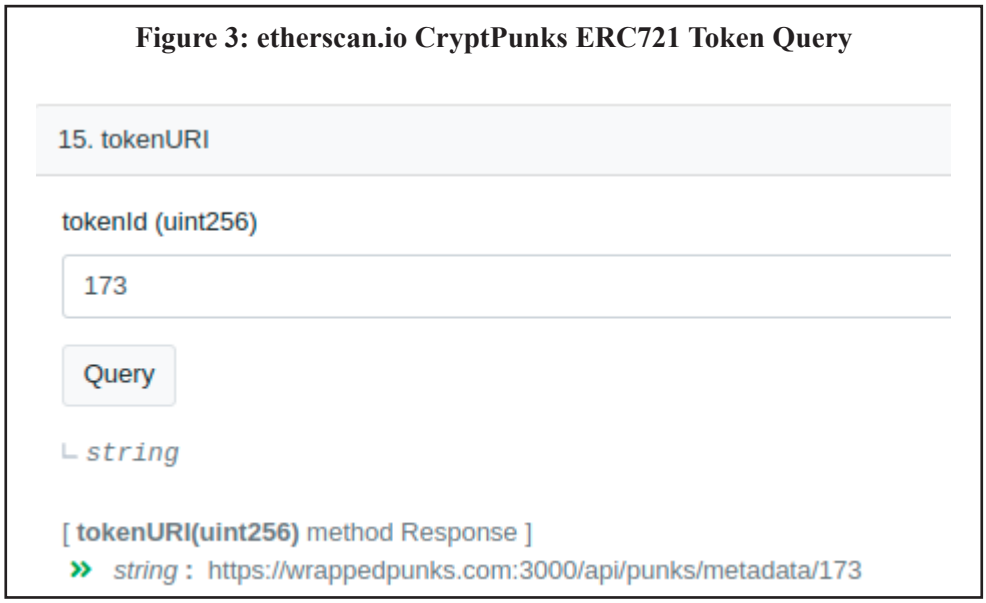


Figure 3: etherscan.io CryptPunks ERC721 Token Query



ERC721

The ERC721 standard[6] defines the methods a smart contract must implement to create and manage the ownership of unique data items known as non-fungible tokens (NFTs). NFTs represent data stored elsewhere (*e.g.*, at a web address) or sometimes the data is stored within the smart contract itself. In TradFi equivalents, an ERC721 smart contract is like a custody bank that holds the unique deed of ownership to a unique item of real property, and sometimes the bank also holds the real property in its vault. As with ERC20 smart contracts, because they have unique addresses represented by cryptographic hashes stored on the blockchain, I define an ERC721 token as being the index of a specific ERC721 contract hash that contains the information required to acquire the data of the token. The data can be anything - a document, an image, a media file, nonsense, or any combination and more.

ERC721 is difficult to understand at the implementation level because it's normally a record of something that is "off-chain," meaning that the data is not on the blockchain and is instead on a storage system of some description. This means that the information in the smart contract is reference/location information, and the retrieval of the actual target data requires additional technical steps. A famous NFT example is the Cryptopunks collection. Figure 3 shows the process to get the image of Cryptopunk number 173 where I need to use etherscan.io to call the function on the smart contract to find out where it is, and then I need to go to the web address that is returned to get the image.

As the NFT standard defines a complex blockchain record keeping system, most NFT trading is done on NFT exchange web applications such as opensea.com that provide a simple user experience to manage the process.

ERC1155

The ERC1155 standard[7] is a newer standard that combines the ability to create any arbitrary number of fungible and non-fungible token types within the same smart contract. This standard was created for activities such as games where many token types may need to be created and destroyed over time, and paying the gas to create a new smart contract for each new token would become prohibitively expensive.

PROTOCOLS AND DAPPS

The ERC20 token and ERC721 NFT standards provide the building blocks for token creation and use that developers can use in their own smart contracts. These smart contracts can range in function from the simple creation and management of tokens, through to complex algorithms and compositions that work across one or more of the smart contracts that implement the standards. The convention is to describe this development activity as "Protocol" development, and

the web applications that interface to the protocols are called "dApps" for decentralized apps. It is the sum of protocols and dApps that defines the DeFi space.

DEFI ASSETS

At the time of writing there are over 515,000 ERC20[8], 65,000 ERC721[9], and 7,000 ERC1155[10] smart contracts on the Ethereum blockchain. The majority of these are irrelevant thought bubbles and most of DeFi is defined by a relatively small number of categories of protocols and their usage. To help build a picture for you of the types of DeFi activities that are occurring, I will explore a small set of examples, their purpose, and the way they work, and show how they interrelate through other protocols.

TETHER STABLECOIN

Tether is an ERC20 token with the symbol USDT that is a US dollar stable coin like USDC. One Tether is designed to represent one USD, and hence promises to not have the volatility of cryptocurrencies in trade due to its USD peg. What's interesting about Tether is that it predates Ethereum and the ERC20 standard having started as an early attempt at storing digital assets on the Bitcoin blockchain by using what equates to a note on a Bitcoin transaction as a reference to a transaction somewhere else. It is now available as an ERC20 token, and is also available on several other blockchains. Tether has, let's just say, an interesting history and the company that manages it is not domiciled in the USA. It is an example of a USD stable coin that people rely on as being asset backed, but it is managed offshore by a company called Bitfinex with dubious provenance and quality, and has been pursued by USA regulators.[11] At the time of writing Tether had 39.8BN USD of ERC20 token value.[12]

USDC STABLECOIN

USDC has already been discussed as an example of the ERC20 token standard. USDC is an example of a regulated U.S. dollar stable coin that is traded as an ERC20 token. It is provided by Circle Internet Financial LLC who is responsible for the asset back guarantee process, and the company is regulated to ensure standards are met. It promotes USDC use as a way to use the Ethereum blockchain as a new payment mechanism, but with old fiat money. It was initially established in the market through a partnership Coinbase, another U.S. based institution that also works with U.S. regulators to ensure that it is in step with U.S. law. At the time of writing USDC had 50.5BN USD of ERC20 token value.[13]

MAKERDAO & DAI STABLECOIN

Now that we have discussed the asset backed tokens of USDT and USDC with their varying pedigrees and standards, we can review a "crypto native" stablecoin that is a "decentralized" token. Recall that USDT and USDC are USD asset backed, which is the antithesis of crypto idealism as crypto assets are not supposed to be controlled by institutions or governments or custody banks. DAI is a U.S. dollar stable coin that is traded as an ERC20 token that uses smart contract programs to manage a peg to the USD. In simple terms, it is a smart contract version of a central bank with a market operations system that manages the process of accepting user's Ethereum deposits into "vaults," which are converted into DAI tokens that the user can then use where DAI is accepted as a payment token. The DAI valuation peg is managed relative to the USD price of Ethereum as indicated by the trades seen on cryptocurrency exchanges.

The MakerDAO that controls DAI is a collaboration of people, organized in cyberspace, that call themselves a distributed autonomous organization (DAO). Let's grant them that claim for now. As a DAO, there is also a MakerDAO ERC20 token issued that represents membership in the MakerDAO, and these tokens are used for voting purposes in the operation of the various DAO committees. MakerDAO is also interesting in that the protocol pays a "yield" to those that "stake" (deposit) their Ethereum into the process, charges fees for those using it, and has a margin loan management facility to leverage Ethereum into more DAI. Whether the algorithm is as bulletproof as the proponents imagine, the MakerDAO liquidity providers fund it in a margin management tail event, or its costs stand up to financial scrutiny, only time will tell. At the time of writing the DAI ERC20 token had 8.7BN USD of ERC20 token value,[14] and the MakerDAO ERC20 token representing DAO ownership was worth 1.8BN USD.[15]

WETH WRAPPED COIN

This may seem counter intuitive, but because ERC20 tokens are hypothecated inside smart contracts on top of the Ethereum blockchain, the Ethereum cryptocurrency is not available in the ERC20 contracts that are built on it. To solve this problem, the concept of "wrapped Ethereum" was created so that Ethereum was also available as an ERC20 token. Through some clever smart contract programming, ETH can be sent by a wallet to a smart contract address, locked, and the equivalent ERC20 WETH token "minted" (created) for use by the sending wallet address. The reverse process is that WETH can be sent into the contract, "burnt" (destroyed), and real ETH sent to the wallet address. At the time of writing, the WETH smart contract developed by RADAR RELAY, an online distributed exchange (DEX), held over $19BN USD of WETH.[16]

COMPOUND

The Compound protocol family and DAO takes ERC20 token deposits, and makes ERC20 token loans. It charges interest on loans and pays interest on deposits. Compound also offers a product called Compound Treasury, which is a partnership with the USDC Token creators to allow USD loans to be made with people using blockchain technology to buy loan assets and take on loan liabilities. Compound also has a DAO that allows owners of the COMP DAO token to vote on proposals to make changes to the compound protocols. At the time of writing, the Compound protocol had over 9BN USD worth of more than 180 ERC20 tokens available for lending,[17] and the Compound Treasury protocol claims to pay a constant 4% APR on USD deposits.[18]

NOUNS DAO

The Nouns DAO Protocol introduces us to the ERC721 standard. Figure 4 shows a Nouns DAO avatar image produced by the Nouns DAO algorithm. Every Nouns DAO token is unique on a set of dimensions known as traits.

Recall that the ERC721 standard is for recording non-fungible, or unique data on the blockchain. This standard has spawned a whole new way of distributing media content on the internet, and also driven its own technological experimentation with ways media are created and monetized. The Nouns DAO is the epitome of this movement as first, it is in the category the Bored

Figure 4: A Nouns DAO Avatar

Apes, CrypToadz, CryptoPunks and CryptoKitties collections; memes that generate eye popping valuations among collectors, and second, it is at the forefront of experimentation with blockchain generated art merged with DAO concepts. The reason it is "pure" blockchain generated art is because each is a unique image that is generated daily by smart contracts from data on the blockchain; it doesn't point to data held elsewhere such as on the interplanetary file system (IPFS) used by most NFT collections to hold their data. This is interesting insofar as it pushes the boundaries of what can and should be done using smart contract programming. However, to me, it is the DAO implementation that is the most interesting and makes it a meme project worth understanding.

The Nouns DAO is a clone of the Compound DAO smart contract that allows owners of the Nouns DAO token to participate in the submission and approval process of Nouns DAO proposals. The daily auction of the Nouns DAO NFT is collected into the smart contract to fund the proposals, and the access to the funds is controlled by a "multi-sig" approval process, which means that a certain multiple of designated signature holders must sign the release of the funds from the DAO to a recipient. At the time of writing, this "trivial" meme project has a treasury of over $69M USD of Ethereum assets in its treasury for the DAO[19] to spend on whatever proposal they can collectively dream up in the DAO discord.com chat room. To date this includes, among other projects, partnering with Bud Light on a new beer advertisement at the 2022 superbowl to include the iconic Nouns DAO glasses,[20] and more recently, providing crowd funding for an indie film.[21] If you want to join the Nouns DAO at the time of writing, the cheapest asking price of a Nouns DAO NFT, which is known in crypto speak as the "floor price," is 67.99 ETH,[22] or more than 207,000 USD.

DEFI EXCHANGES

Now that I have introduced some of the varied types of assets created using the ERC20 and ERC721 token standards, I can move to the DeFi exchanges on which these assets are traded. It is worth noting that because many exchanges issue DAO tokens, DeFi exchanges are also ERC20 assets in the same way the TradFi exchanges are also listed companies. Most people are familiar with cryptocurrency exchanges such as Coinbase, which are known as fiat exchanges because it is where cryptocurrencies are exchanged for fiat currency, and vice versa. These exchanges are companies that are intermediaries between the banking system and the blockchain systems, and they are a necessary point of centralization for those that want to move back and forth between the cryptocurrency world and traditional fiat currency world. They are also known as "fiat bridges" with all the correct connotations of something that can be controlled and have toll collectors. A DeFi exchange is called a decentralized exchange, or DEX, because in theory at least, they are a system of smart contracts and processes that are executed on the blockchain and hence decentralized without any involvement from any centralized service provider.

0x PROTOCOL

The initial ERC20 DEX model was a traditional order book exchange where bids and offers could be recorded and settled through a smart contract that managed the order book and settlement. These contracts worked in theory, but they have the undesirable quality that you have to pay gas in Ethereum every time you execute the smart contract to make an offer, place a bid, cancel an order, or settle a trade. This cost became prohibitive as the price of gas rose as more people competed to use the blockchain and the miners put up gas fees to benefit from the demand. Several alternatives were tried and some initial success was achieved by DEXs such as 0x who solved the problem by moving the order book "off-chain" onto another decentralized protocol that is based around the idea of "relayers" who replicate trade messages to each other. The off-chain transactions are bonded to the Ethereum blockchain through a technique known as "state channels" which are a transaction that marks a fork off the chain to manage an order book across the relays, with the fork finally joining back at a transaction on the chain at a later time on completion of the order book process. 0x was an early pioneer in using fee structures to reward liquidity makers and relay operators through a share of the fees from liquidity takers.

UNISWAP PROTOCOL

A major innovation in the ERC20 DEX space arrived

when the Uniswap Protocol[23] was introduced. The Uniswap protocol is a suite of smart contracts that creates what are called "liquidity pools" of pairs of assets where the price is maintained by the "Constant Product Market Maker Model." The concept was originally proposed by Vitalik Buterin, the founder of Ethereum, in a reddit post[24] where he suggested that DEX models should operate like blockchain "prediction markets" aka blockchain gambling protocols. In this model, if you have a pool of the asset pair x and y of certain quantities and a constant k, then using the simple formula x * y = k to maintain equilibrium means that prices go up and down based on the amount of x and y added to or subtracted from the pool in a swap of one for the other. The benefit of this model is that market makers are incentivized to create and join pools of pairs at fee levels in a competitive way in advance of bids, ensuring that liquidity is always available at a price for any pairs for which there are market makers.

At the time of writing, the Uniswap model, which is now in its 3rd iteration says it has performed over 921BN USD in trade value from over 94M trades.[25] The Uniswap governance DAO token, called UNI, has a total USD equivalent value of 9.7BN.

OPENSEA

The final exchange I will explore is the Opensea ERC721 NFT exchange. Opensea is part centralized like a cryptocurrency exchange for NFT creation and market making, but once a sale is complete it settles "on-chain" and ownership becomes decentralized by creating or transferring an ERC721 Token to the successful wallet through a smart contract known as the Wyvern Protocol. The Wyvern Protocol allows any ERC20 token, or a combination of many tokens to be exchanged and settled on-chain for the purchased ERC721 token. Opensea is the largest NFT exchange and was reported by Forbes as having 3.4BN USD of volume at the peak of the NFT boom of 2021.[26]

It is worth noting that Opensea is somewhat of an iconoclast in the DeFi space as it is a private company that does not present itself as being a protocol developer as it opportunistically picked up the open source code for the Wyvern protocol and implemented it as-is, and nor has it issued a DAO token.

THE METAVERSE

Any analysis of the DeFi phenomenon would not be complete without a discussion of the metaverse. In simple terms, the metaverse describes the class of virtual gaming spaces where characters build and interact in a 3-dimensional virtual environment. These worlds are also rapidly moving into XR (x Reality) environments where XR means either fully virtual reality (VR) environments inside a headset, or augmented reality (AR) environments where the real world is augmented visually with virtual worlds through special glasses that combine the two in real time. There can be as many metaverses as there are computer games - an unlimited number that is only bounded by imagination and capital. Some popular projects are Decentraland, Nakamoto, Epic Games and Cryptovoxels. Facebook has renamed itself "Meta" in advance of participation in the metaverse phenomenon, however, they are yet to launch their own version of a metaverse.

Figure 5 is a view from the Cryptovoxels metaverse that shows how the metaverse is the perfect expression of DeFi culture. The blocks of land are called "parcels," which are created and auctioned as NFT tokens on NFT exchanges. Owners can build and decorate their own virtual buildings and the creation of NFT art galleries to show personal collections is a favorite pursuit. Users can also create and sell Cryptovoxels wearables (digital clothing, jewelry etc.) as NFTs to users that want to dress up their avatars that exist in the Cryptovoxels metaverse. DeFi initiatives also promote themselves in the metaverse as can also be seen in Figure 5 which depicts a billboard for a Ukraine fund raising DAO. At the time of writing, the total value of Cryptovoxels parcel sales on opensea.com is over 74M USD, and wearables sales are over 800K USD. [28]

DISCUSSION

DeFi is yet another cryptocurrency Rube Goldberg machine that is extraordinary for many reasons, not least of which is that it came into existence in the first place. There are many aspects of DeFi that I have not covered including the application of derivatives to DeFi assets, collective investment programs that include DAO fund raising, and the cornucopia of applications that integrate across multiple protocols. I have also avoided bringing

Figure 5: A View from the Central District in Cryptovoxels.com[27]

in the many DeFi specific terms such as staking, yield farming, liquidity mining, tokenomics, and technical changes such as proof of stake, just to name a few. These distract from my central narrative which is that DeFi is not a finance space, it is a self referential meme space that also inherits the rule breaking culture from the underlying cryptocurrencies that spawned them. Nevertheless, the technology innovations and social dynamics arising from this activity will prove to be important over time.

THE MEME SPACE

Table 1 shows the top 5 ERC20 tokens or ERC721 token collections that were listed on the Compound, Uniswap, and Opensea exchanges at the time of writing.

What can we conclude from this table? Simply that the DeFi space is a money go round of DeFi tokens chasing DeFi tokens. I am not being critical of DeFi developers in this observation; I see it like the gamer space, which

Table 1: Top 5 Tokens by DeFi Exchange

Compound	Uniswap	Opensea
Aave (lending protocol)	WETH	CryptoPunks
Basic Attention Token	USDC	Bored Ape Yacht Club
Compound DAO Token	Tether	Mutant Ape Yacht Club
DAI Token	Wrapped Bitcoin	Art Blocks Curated
WETH Token	DAI	Decentraland

is an important and profitable industry that adds value to its users and spins off technology into other areas. For example, the AI engines in gaming systems are at the leading edge of physics simulators, machine learning, and decision making, and the terraforming and visualization algorithms push graphics development with crossovers into creative, industrial, and defense industries. However, as a meme driven experiment in the use of blockchain technology, DeFi is constantly enveloped in the miasma of relying on pyramid scheme dynamics where the early promoters are taking advantage of the late entrants who are attracted to the promise of a gourmet banquet only to find they have been lured into a lobster pot. For personal DeFi participants, the first NFT they purchase should be the sign - caveat emptor.

I am highly critical, however, of those who say this is legitimate finance and that any of these tokens are investment grade. As I discussed in my previous paper on cryptocurrencies, the risks of the blockchain cryptocurrencies are still so high as to require a vigilant approach for short term investors, and I believe that anyone who acts as agent and not principal would be irresponsible to propose that cryptocurrencies are a prudent long term investment suitable for a retirement fund. The risk of participation for prudent institutional investors in the DeFi experimentation occurring on top of cryptocurrencies should be imponderable. Of course direct investments in startups involved in the DeFi space, or funds that do so, is completely reasonable to me as that is the normal process of participating in the formation and growth of startups within the risk management strategy of investing in a portfolio of startups.

THE RULE BREAKING

The USD stablecoin phenomenon certainly has the attention of lawmakers. Circle, the company that provides USDC has disclosed it has been subject of SEC subpoenas.[29] The New York Attorney General banned Tether and Bitfinex from operating in New York as "Bitfinex and Tether Deceived Clients and Market by Overstating Reserves, Hiding Approximately $850 Million in Losses Around the Globe," and Coinbase stopped its project to offer its crypto based "Lend" product due to the threat of action from the SEC.[30] Similarly, it is not just stablecoins that have the attention of the law with the SEC reported to be investigating Uniswap Labs, the maker of the Uniswap exchange and issuer of the UNI DAO token.[31] The self declared independence from securities law by calling a project a DAO is a very thin fig leaf indeed when the websites, dApps and smart contract execution processes are done by companies incorporated under the securities law they hope will protect their IP and massive fiat denominated valuations, all the while wishing to profit from operating services that ignore the same laws. A bill known as the "Stablecoin Innovation and Protection Act" has also been tabled in congress.[32] The DeFi space may indeed be ahead of itself on regulation, but rest assured that the SEC and other regulators and lawmakers will work slowly but surely to catch up.

TECHNOLOGICAL INNOVATIONS

It is without doubt that cryptocurrencies have created a Cambrian explosion of creative and experimental digital lifeforms, many of which will die, but much of the DNA of these projects will also be carried into the future. The innovations I have described; the EVM, Solidity, the ERC standards process, and the decentralization of the payment system out to the end user via crypto wallets, have together created a huge new industry of new skills and new thinking about ways to do things. The millennial generation of software developers now have this technology and thinking built into the core of their intellectual and commercial zeitgeist, and in the same way that the dot com era boomed and busted but left us with a new way to think about moving everything in the world online and then to mobile applications. I believe that the future is now in the hands of a new generation predisposed to thinking about everything as decentralized and "on-chain". Investment decision makers may be unwise to jump into the current DeFi boom, but they would also be unwise to ignore that it portends a new way of doing business. DeFi is yet another new play based on the old script of the destruction of intermediaries, introduction of new experiences, and the realignment of capital based on new technological innovations. Those in the media, finance, and social spaces ignore what is happening here at their peril.

DECENTRALIZED SOCIAL DYNAMICS

The final dimension of the web3 phenomenon I wish to

touch on is the social dimension. Imagine if you will that some engineers and scientists came together to build a biosphere. Some were preppers who thought the world was going to end, others were visionaries who wanted to have a go at building a new world made of free and sunlit uplands, and some were just really good at building biospheres and were willing to do it for the fun of it. These misfits fought and grumbled and looked like lunatics, but build it they did, and they succeeded. The biosphere was created, it works better than anyone could have imagined, and it provides a whole new environment for new life to thrive. Initially the biosphere builders inhabited their creation, but they didn't have the imagination or the skills to make the stuff of life - landscapes, buildings, parks, lifeforms, art galleries, music, and comedy stores. Soon they found that the biosphere was being colonized by the people who could do those things, and the culture started to change. Diversity, inclusion, creativity, irl (in real life) parties; all those things that were not part of the culture that built the biosphere suddenly became a cultural phenomenon within the biosphere.

This is how I relate to what is happening around culture and web3 projects. I call it "Decentralized Social" where there is a whole new iteration of norms and values integrated with advanced technology, social platforms, open source software, and development practices that are playing out in spaces that TradFi and different generations may not see. People call cryptocurrency "millennial gold", but it is also enabling a "millennial world" in which they are spending their gold in ways we cannot imagine, and for experiences we cannot understand. There is something going on here, and it's going to be important.

CONCLUSION

What I have described in this paper is a virtual world created by computer programmers and colonized by cultural phenomenons that are monetizing itself through virtual tokens and then turning itself over and over and over and calling the process "finance." They have created DeFi as the financial fabric of the metaverse; it's not real and it's not finance, and oftentimes it is absurd. The extraordinary valuations are based on the current conversion rate of cryptocurrencies to the USD fiat currency, and it is worth remembering that even that conversion rate may not survive the test of time. This truly is the second moment of a first order effect that may itself disappear. But most digital technology innovations start as projects among idealists dreaming of unrealistic futures where everything changes, while the realists dream of unrealistic futures where nothing changes. Traditional realist thinking would say it should have never started, let alone flourish and threaten to become a new force in the world of TradFi, but then the same can be said about cryptocurrencies where traditionalists said they would never succeed or be taken seriously.

And how did that prediction work out?

EPILOGUE

Two recent events highlight just how dynamic and fast paced the environment is around cryptocurrencies. The first is the appalling invasion of an independent Ukraine by Russia. When the invasion began, the web3 community immediately swung into action and the UkraineDAO, whose organizers included the Ethereum founder Vitalik Buterin, raised over 8M USD for use in Ukraine.[33] This raising was all done "on-chain" in cryptocurrency, and the use of the funds is controlled by the DAO members. On the flip side of the virtual coin, with the western world also immediately imposing harsh sanctions on Russia, including the sanctioning of individuals, corporations, and banks, the focus moved to cryptocurrencies as being a risk as a way to circumvent sanctions for Russian oligarchs and companies. Both of these are indicative of how cryptocurrencies are now an item for discussion in global events, and that they will increase in both their scrutiny and importance.

This also leads to the second important development which is the White House releasing President Biden's "Executive Order on Ensuring Responsible Development of Digital Assets."[34] My key read of this document is that we will see a proposal to create the ultimate USD stable coin which is a central bank digital currency (CBDC) issued by the USA government, the environmental issues of cryptocurrencies will receive intense focus, and there will be proposals by the security apparatus that will try to tame free cryptocurrencies. This attempt at controlling cryptocurrencies will be in direct tension with the desire to keep the USA on the leading edge of innovation. I recall the 1990s fracas between the government and industry about the NSA

proposed "Clipper Chip"[35] that allowed secure internet transactions, but could ultimately be read by law enforcement and security agencies. The Clipper Chip proposal failed; only time will tell how this process plays out for cryptocurrencies.

ENDNOTES

[1] "Sushi Restaurants in the US - Market Size 2005-2027, IBIS World, 2021 https://www.ibisworld.com/industry-statistics/market-size/sushi-restaurants-united-states/

[2] https://opensea.io/collection/cryptoadz-by-gremplin?tab=activity

[3] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System,"https://bitcoin.org/bitcoin.pdf.

[4] https://eips.ethereum.org/EIPS/eip-20

[5] https://etherscan.io/address/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48

[6] https://eips.ethereum.org/EIPS/eip-721

[7] https://eips.ethereum.org/EIPS/eip-1155

[8] https://etherscan.io/tokens

[9] https://etherscan.io/tokens-nft

[10] https://etherscan.io/tokens-nft1155

[11] https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal

[12] https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7

[13] https://etherscan.io/tokens/label/usdc

[14] https://etherscan.io/token/0x6b175474e89094c44da98b954eedeac495271d0f

[15] https://etherscan.io/token/0x9f8f72aa9304c8b593d555f12ef6589cc3a579a2

[16] https://etherscan.io/token/0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2

[17] https://compound.finance/

[18] https://compoundtreasury.com/

[19] https://etherscan.io/tokenholdings?a=0x0BC3807Ec262cB779b38D65b38158acC3bfedE10

[20] https://twitter.com/budlight/status/1490641491622043650

[21] https://decrypt.co/97862/nouns-dao-backs-nft-crowdfunding-effort-for-indie-film-calladita

[22] https://opensea.io/collection/nouns

[23] https://uniswap.org/whitepaper-v3.pdf

[24] https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/

[25] https://uniswap.org/

[26] https://www.forbes.com/sites/jeffkauflin/2021/11/23/what-every-crypto-buyer-should-know-about-opensea-the-king-of-the-nft-market/?sh=4fe788a22f89

[27] https://www.cryptovoxels.com/play?coords=SE@7W,11S,3U

[28] https://opensea.io/collection/cryptovoxels

[29] https://www.sec.gov/Archives/edgar/data/1876042/000110465921122565/tm2124445-1_s4a.htm

[30] https://blog.coinbase.com/the-sec-has-told-us-it-wants-to-sue-us-over-lend-we-have-no-idea-why-a3a1b6507009

[31] https://www.coindesk.com/policy/2021/09/03/sec-investigating-uniswap-labs-report/

[32] https://gottheimer.house.gov/uploadedfiles/dd._stablecoin_innovation_and_protection_act_of_2022.pdf

[33] https://fortune.com/2022/03/31/ukraine-dao-crypto-donations-vitalik-buterin/