**WEB3 BRIEFING:  
What are Blockchain, DApps, and The Metaverse?**

By Glacial Lake Solutions

3/10/2022

**Intro**

The internet began as Web1 (inception -> 2005), a series of documents with hyperlinks between them (aka websites) in which http protocols allowed the user to enter URLs and visit documents. Web2 (2005-2020) was characterized by centralization of data, applications, and the deterioration of privacy in data. In other words, as centralized applications were adopted (facebook, google) the user data from the services were bought and sold without participation from the user - an essentially exploitative, zero-sum relationship. The landscape of internet technology is changing again with the innovation of blockchain technology and this seachange is called Web3. From 2020 onward, blockchain adoption has accelerated beyond initial internet adoption between 1990 - 2005. [[1]](#footnote-0) Web3 is defined as an internet of blockchains. Metaverse is defined as the totality of interoperable blockchains - type I decentralized applications (DApps) - with type II and III DApps built upon them that a user may port data between seamlessly. The easiest way to understand this is with DeFi or decentralized finance DApps which may be Type I, II, or III. For example: smart contracts are built into Ethereum’s blockchain (type I) and then DApps that use these smart contracts in building blocks are type II (such as decentralized exchanges or DEX).

**PART 1**

What is blockchain?

**P1 - §1:**

BLOCKCHAIN: OVERVIEW AND BASICS

A blockchain is a digital record-keeping method which employs a structure of groups of timestamped data entries (blocks)(which could represent any kind of data record) that are linked together sequentially into “chains”. The link between blocks is established cryptographically, wherein each new/leading block contains a cryptographic hash (an algorithmically generated [via a mathematical function, i.e. input-to-output] bit array [a group of groups of alphanumeric characters] of a fixed size which has a unique mathematical relationship to some/any given set of input data) of the preceding block in the chain. Typically this data is stored in a tree-like structure called a Merkle Tree (hash tree), which has the benefit of being a very efficient way (particularly when compared to a simple list) to store chained/linked cryptographic hashes due to the reduced number of mathematical calculations which need to occur to verify that any given entry in the structure is a valid one.

**P1 - §2:**

BLOCKCHAIN: IMPLEMENTATION (Distributed ledger, network, consensus)

While a blockchain itself is nothing more than a “way” of storing data, they are typically, and most effectively, used in “peer-to-peer” networks where many independent computers/users on a network (by virtue of an internet connection and a shared set of communication and storage protocols) can collectively and redundantly (every node of the network “has a copy”) store the contents of what is called a “distributed/public ledger”; which itself may contain the complete history of transactional and ownership related data about both digital objects (cryptocurrencies, contracts, documents, and tokens [generally: fungible and non-fungible]) and digitally-represented physical objects (through ‘tokenization’).

Critically, the protocols on a blockchain network support a “consensus mechanism” (which can be one of many different kinds) which generally speaking allows the participants in the network to collectively and trustlessly (without knowledge or proof of the identity or motivation of the other participants) verify the data that is being committed to the blocks. Typically these consensus mechanisms will employ some kind of ‘cost’ (computational time/energy, staked funds, etc.) incurred by the participants which prevents (or at least severely limits) the ability of any single participant from controlling a majority of the network's nodes, and therefore its verification capacity. Many other cryptographic methods are also employed to ensure tolerance to errors, false reporting, and malicious attacks which would ultimately seek to commit false/invalid data to the distributed ledger.

**P1 - §3:**

BLOCKCHAIN: CRYPTOCURRENCY

In the specific case of cryptocurrencies, blockchains are used generally to store the data which comprises a publicly accessible distributed ledger (all the data, while ‘anonymized’ is quite literally viewable by anyone who wishes to look). This ledger primarily includes records of transactions of certain amounts of fungible tokens (digital data objects that are identical to each other) between participants on the network which are referenced by ‘wallet addresses’ (unique string of numbers and letters). In order to verify all of these transactions (and most importantly to prevent the “double-spending” of the tokens) the participant nodes of the network run the aforementioned network protocols which comprise the consensus mechanism (proof-of-work, proof-of-stake, etc.). By doing this, the ledger data which is written onto new blocks of the chain is collaboratively verified/validated. This process is referred to as mining, because a small amount of the kind of tokens which are used on the network are given as a reward to the node participants for their efforts. The rewarded tokens are in some cases literally created anew during this process, and in other cases garnered as a fee from those who are transacting across the network, and redistributed to those who are paying the cost (computational or otherwise) to “secure” (verify through consensus) the network.

**P1 - §4:**

BLOCKCHAIN: OTHER USES AND FEATURES

One of the original proposed uses of blockchains was as a method to ensure that the timestamps on documents in a given shared database could not be tampered with. This is still a valid use-case today, and generally speaking blockchains, when used on a network and verified through consensus mechanisms, are a very good way of storing, distributing, and securing the data and metadata related to any kind of document or data-structure. In this way, blockchains can do a lot more than encode transactions of fungible tokens. For example, a blockchain can support a kind of protocol between two or more agents called a Smart Contract, which allows terms of engagement (including any number of stipulations relating to elapsed time, the transaction of funds, or the fulfillment of specific criteria) to be automatically executed and enforced, without the need of a trusted third-party. Additionally blockchains can support the verification of ownership and transaction of data objects called “non-fungible tokens” (NFT) which have an asset-like quality similar to cryptocurrencies (fungible tokens) but are distinct in that they contain/encode entirely unique pieces of data, and are therefore not identical to each other.

**P1 - §5:**

BLOCKCHAIN: CONCLUSION

Generally speaking, blockchain technology is considered to be advantageous in the cases in which it is employed, because it is “decentralized”. In other words, it does not rely on any central authority to verify and store the ledger records. This is particularly salient in what are called “permissionless/public” blockchains (where anyone can participate and use the network and its resources). However, “permissioned/private” blockchains also exist and can be a powerful tool for private enterprise and governments who may need to track and secure records about any number of complex and interrelated sets of data (e.g. supply chains, etc.). In the private case, the “trustless” nature of the consensus mechanisms that secure the data on the network is not necessarily very important (since the nodes which do this are typically owned and operated by the private entity itself), but the decentralization of the records across many nodes in the network is still a huge advantage in many different cases with regards to data security, validity, and fault/error tolerance.

**PART 2:**

What connects to blockchain?

**DApp: Decentralized Application**

A DApp is an application that runs on a blockchain. Specifically, the DApp’s code is stored and executed on a blockchain network and it is therefore able to operate entirely autonomously (without the need for a central server or administrator). Usually DApps involve the use of Smart Contracts to manage and execute user interaction, and ultimately to provide useful functionality. DApps are decentralized by nature and are therefore also ownerless, instead ownership (which could afford many different things depending on the DApp) is granted cumulatively to those who hold the tokens (could be a cryptocurrency, governance token, etc.) which are distributed/produced by the DApp, in a way that is similar to a company share. DApps are classified generally into 3 “Types” (Type I, Type II, and Type III). Type I DApps run on their own blockchain network, and it is the protocols of that network which constitute the code of the DApp itself, examples include: Bitcoin, Ethereum, etc. Type II DApps are built on top of Type I DApps (analogous to an application which can only function by virtue of an operating system running in the background). A Type II DApp will have its own tokens (for governance, trade, and operation) but is fundamentally tied to the Type I DApp that it is built upon because the Smart Contracts which enable its functionality are stored and executed on the blockchain of the Type I DApp. Finally, Type III DApps use protocols which run on top of the protocols of a Type III DApp, in much the same way as Type II relates to Type I. It is the case that this Type classification could be extended indefinitely, as DApp protocols and functionality could be built in successive layers on top of lower level infrastructure ad infinitum (in much the same way that software implementations form ‘stacks’), however in practice each new layer is ultimately relying on the finite resources and throughput of the blockchain of the Type I DApp all the way down at the root of this hierarchy, thus physically limiting the total number of DApps that could run on a single blockchain network (or at the very least inflating the cost so dramatically that it becomes unviable, and far more practical to build a whole new first layer from scratch).

**DeFi: Decentralized Finance**

DeFi is a general term to that refers to the entire nexus of Decentralized Economy (including blockchains, cryptocurrency, NFTs, Smart Contracts, etc.) and all of the more traditional instruments and systems of Finance (including security trading, margin trading, fund/asset investing, lending & borrowing, insurance, etc.). Typically, Decentralized Financial systems and instruments have the advantage of operating as DApps which run as code on a blockchain, and are therefore able to avoid government regulation, including IRS & SEC oversight. DeFi apps by their very nature as part of the decentralized economy are able to offer a variety of new and innovative forms of finance (ways of making money), including: Staking (which offers rewards and is required for proof-of-stake consensus), Providing Liquidity (adding funds to pools on decentralized exchanges in order to receive transaction fees as a reward), and various kinds of high-speed lending & borrowing (which are only possible through the use of Smart Contracts). Much of the world of Decentralized Finance is NOT provided by private organizations but is instead managed by what are called DAOs: Decentralized Autonomous Organizations, which are themselves DApps.

**DAO: Decentralized Autonomous Organization**

A DAO is a kind of organization that is implemented in code that is stored and run on a blockchain. Critically, DAOs are entirely transparent (the code which contains its transaction records, programmed functions, and rules of operation is viewable by anyone), and they have no central governing authority or ownership-entity (person or otherwise). Instead DAO’s ownership is distributed through shares tied to “governance tokens” which can be traded like any other crypto-asset, and which in many cases confer voting rights to token holders when any change to the DAO is proposed and put to a vote. Apart from being acquired through trade on an exchange, DAO governance tokens are often awarded to users who invest in the DAO in some way, for example: through providing liquidity (in the case of a DEX), investing capital as a lender, or even through interactions with a DeFi game. DAOs may essentially be a single DApp (decentralized application), or they could be an entire platform containing an ecosystem of multiple DApps.

**DEX: Decentralized Exchange**

A DEX is a kind of DApp which allows users to trade cryptocurrencies, in the form of a “swap” from one particular asset to another (Ethereum-to-Bitcoin, Litecoin-to-USDTether, DAI-to-SHIB, etc…). What makes these distinct from a “centralized exchange” (like Binance, Coinbase, or the New York Stock Exchange) is that no ‘order-book’ is necessary to facilitate trades between actual buyers and sellers, and therefore no central authority is required in order to calculate and confirm the settlement of these trades at a particular price. Instead, in a decentralized exchange, “liquidity providers” (people who have various currencies on hand, and who usually intend to hold them for some amount of time) can collectively add to ‘liquidity pools’ which are organized to hold tokens in the aforementioned swap pairs (any two cryptocurrencies can be paired together, and it is up to the DEX in question to support a given pair). A liquidity pool is designed to allow a trader to swap their tokens for the other token in the pair, WITHOUT the need for another trader wanting to perform the opposite trade at the same price (which is normally required to facilitate an exchange in the ‘centralized’ regime). The liquidity pool is able to facilitate this kind of ‘automated’ trading by also adjusting the price of the assets it contains as the supply of those assets fluctuates. Specifically, liquidity pools use a mathematical formula called a ‘constant product automated market maker’ which REQUIRES (by automatically changing the trade price of the tokens) that the overall value inside the pool remains constant even as traders add and remove tokens to either side of the pair. Liquidity providers are always required to put up equal amounts (by value, as determined by the current trade price) of each token in the pair, and therefore the pool as a whole also always contains equal amounts (by value) of each token in the pool pair. Liquidity pools DO NOT require trade price information from an outside source like another exchange, and instead the price is entirely regulated mathematically, based on the volume of contained tokens. Because of the ‘automated’ nature of a decentralized exchange, there is some opportunity for arbitrage between certain pool pairs when, for instance, the trade price of only one of the tokens in the pair changes dramatically, while the other stays the same, or changes in the opposite direction. This will lead to something called “impermanent loss” for the liquidity providers, as some amount of the tokens that they are providing liquidity for can be sold/swapped out by the automated market maker for some price below the going rate (relative to other exchanges). In other words, the liquidity providers incur a “loss” by virtue of some amount of unrealized profit as a result of the token price change. While a small amount of impermanent loss happens all the time, it is for the most part greatly offset by the pool fees which are awarded by pool-share-percentage to the providers.

Generally speaking, decentralized exchanges are a critical part of the world of decentralized finance. Liquidity is necessary to facilitate commerce and capitalization in the crypto-economy, and liquidity providers are financially rewarded for their service through the pool fees garnered on every swap. While a private organization could certainly provide automated markets through the use of liquidity pools, most DEXs are themselves decentralized applications running as code on a blockchain, and in most cases are considered DAOs (decentralized autonomous organizations).

**Blockchain Games**

Since 2017 (marked by the release of CryptoKitties) a number of games and gaming platforms have attempted to implement/incorporate blockchain technology to varying degrees. Some simply involve the use of cryptocurrencies for the purchase of in-game goods, where others may include NFTs, as in-game items, character avatars, or other kinds of assets/objects which can affect gameplay mechanics. Often games in this category are referred to as “play-to-earn” as they are typically intended to actually allow players to make money (in the form of cryptocurrency or an NFT) and to capitalize on that value in a variety of gamified ways (usually resulting in newly minted tokens of some form or another). Many blockchain games are in some sense “free-to-play” (apart from what could be a considerable initial buy-in to purchase an NFT for in-game use, or some amount of the associated cryptocurrency) and developers will usually recoup their costs and turn a profit from transaction fees instead. Generally speaking, blockchain games have received a huge amount of criticism from all sides (despite many undeniably popular successes), where most objectors tend to think of these kinds of games as “exploitative”, “lacking in real entertainment value”, “scammy”, and “no different from gambling”. However, most proponents of this new media paradigm see the nexus of gameplay and finance as not only a logical, valuable, and inevitable consequence of blockchain technology, but also as one of the first small steps into a whole new world of online interaction based on blockchain networks, supporting all sort of activities including: work, play, education, and communication… Web3.

**AR/VR: Augmented Reality & Virtual Reality**

AR and VR refer to two emerging human-computer interface categories which are both designed around interaction models that involve multiple sensory modalities (immersive visual display, as well as auditory, haptic, and proprioceptive forms of both input and output). Specifically, Augmented Reality refers to any interface which uses real-world visual information (as live digital video on a display, or as seen by the naked eye through a transparent display) which is then “augmented” by a digital overlay that is coordinated with the environment in real-time. Often AR involves the insertion of 3D and 2D digital objects & image-filters into the environment that is being displayed using motion tracking software systems (these systems usually include cameras, accelerometers, and possibly other forms of spatial sensing like LIDAR), but as previously stated they can also include auditory and haptic feedback as part of the real-time augmentation. On the other hand, Virtual Reality is underpinned by an entirely computer generated visual environment displayed through a VR headset which uses specialized optics to present an image that covers the user’s entire field of view. Virtual Reality also involves data captured by cameras and accelerometers, most often to translate real-world motion (of head position/orientation, hand motion, and the surrounding environment) into virtual motion manifested by changes in the computer generated environment. AR and VR are overlapping interface typologies, insofar as both use the motion and orientation of the user to continuously update the visual display in order to simulate a coherence between environment (which is either entirely or partly computer generated) and occupant (which is always based on a real user, and then projected virtually as a point-of-view [virtual camera position] or avatar). Since their earliest iterations, both AR and VR have been embraced and pioneered by many developers in the video game industry, however, many other applications have been proposed and prototyped in fields and industries both in and beyond entertainment, including: design, construction, telecommunication, logistics, manufacturing, commerce, film & TV, visual art, education, social networking, navigation, war, and even scientific research.

*The Metaverse*, a portmanteau of “meta” and “universe”*.* AR and VR interfaces are integral to the speculative transformation of the world wide web into a new paradigm known as “the metaverse”. The term is originally from a science fiction novel from the early 90’s (*Snow Crash* by Neil Stephenson, 1992) which described a near future instantiation of the internet that was entirely mediated by virtual reality, this led to a unification of all parts and ‘locations’ of the world wide web into one semi-continuous virtual geography that was made to be spatial and traversable. This metaverse environment, being a simulated plane of reality complete with real-time communication between virtual instantiations of users (avatars), could host virtual economic activity that was entirely supported by the resources and demand contained within the virtual world. The “virtual world platform” *Second Life* was one of the earliest realizations of this concept, but it predated any even remotely viable (commercially) form of Virtual Reality and was therefore only ever mediated through a traditional web browser on a flat display. Recent advances in commercial VR technology have reinvigorated the interest in this kind of web development.

Metaverse applications and platforms have not yet found complete integration with the space of Web3/DeFi applications and platforms, however the potential synergy is palpable to many involved in these industries, where some would argue that AR/VR platform development on the web will necessarily be built on top blockchain technology and DApps. In the future, the following categories of service apps will definitely be connected to blockchains in some way, usually in the form of app-specific currencies and/or app specific DAO governance tokens; user data will be stored on blockchains and interoperable with other apps. These apps do not necessarily need to be DApps because they can still be centralized and be on blockchains. If these apps are coded with Smart Contracts, however, then they would be considered DApps. The following are short explanations of the categories of service DApps, excluding finance (as discussed above) and B2B service categories besides remote office spaces such as supply chain management.

* + Workspace
    - Offices

Remote work enabling environments with features for project collaboration

* + - Schools

Remote learning environments with features for teacher insight

* + Socialspace
    - Social Media

Remote social environments with features for interaction

* + - News

Remote viewership environments with features for freedom of speech

* + - Experiences (clubs etc.)

Remote environments with features for interaction that are not necessarily tied to their own networks, but can be inside of social media platforms

* + Playspace
    - Entertainment
      * Story experiences

Remote environments with features for experiencing certain things (horror stories, empathy museums, etc)

* + - * Games

Remote environments with features for playing single-player and multiplayer games

* + - Wellbeing
      * Fitness

Workout

* + - * Mindfulness

Meditation ([Calm](https://www.calm.com/), Flow, Guided Meditation, etc)

Yoga ([YogaVR](https://www.oculus.com/experiences/quest/4828252637184827/))

* Healthcare

User health data from tech (apple watch, sensors etc) visible to the provider interface in VR settings called **Decentralized Healthcare Centers** ([deHealth](https://www.dehealth.world/) etc) where patients can receive remote care, but where a doctor can analyze a patient’s data in real time via tech. These Decentralized Health Centers will run on their own cryptocurrencies and can even be governed by DAOs.

* Immersive rehabilitation (Penumbra)
* Immersive doctor visits

All of the above service types may be turned into platforms and require their own tokens to participate in, which makes them DApp viable, able to be turned into DApps and potentially operated via DAOs.

**END OF BRIEFING**

**PROPOSAL:**

**Ontological Views on Web3 Briefing**

What are the spectral values of ontological entities that can be fit into DApps, Metaverse, and DeFi protocols? In other words, what are the requirements for joining this space, and how do we turn something that doesn’t meet the requirements into something that does?

1. [chaindebrief](https://chaindebrief.com/cryptocurrency-adoption-curve-is-the-fastest-in-human-history/#:~:text=Similarly%2C%20for%20blockchain%20technology%20and,Internet%20in%20the%20late%201990s.&text=With%20crypto%20users%20growing%20at,technological%20adoption%20in%20human%20history.) [↑](#footnote-ref-0)