Crypto Market – The Good, The Bad and The Ugly!

M. Mahdavi
December 2022

Collage by M. Mahdavi

It was just a year ago (November 2021) when crypto prices were at an all-time high and the industry seemingly couldn't have been hotter. It was all going great until it wasn't…

Starting with the implosion of FTX exchange, today, investors are wondering if this is the tip of the iceberg?

There are two scenarios. One would suggest that recent meltdowns is the tip of the iceberg, and we are witnessing the collapse of the crypto industry. You could be in this camp and would have lots of evidence to point to. Another viewpoint would be that the crypto ecosystem is much more complex than what we see in the form of this year's

meltdown and that this is part of the evolution of the industry. There is evidence for this scenario as well.

The title of the article is a telltale of how we can arrive at an answer to this question:

The Good… Crypto market is burgeoning with innovations that can impact multiple industries from pharma to supply chain to cyber security to next generation of internet (web3.0) and to the next generation of financial systems. So, from this vantage point, the crypto technology stack and may of its applications (like DeFi, Supply chain, cyber identity, etc.) will stay and grow albeit, at slower pace due to the recent market meltdowns. After all, the internet didn't go away when the dotcom bubble burst and the likes of Amazon emerged as killer apps.

The Bad…A sector of the crypto market represents crypto lending and borrowing firms (like a shadow bank for crypto). These firms were very attractive to investors since they paid anywhere from ~8% to triple digit interest rates on the deposits! It all works well in the booming crypto market with astronomical valuations…until it is not. As it turns out, collateral for the interest payouts were composed of other made up cryptos! So, once there is a sign of market weakness and a run on the bank, there is no money for the lenders and so a death spiral. This type of chain reaction, not unique to the crypto market, affected several crypto lenders like BlockFi, Voyager Digital, Celsius Network and others. These companies were the market darlings with billion-dollar valuations, thanks to the venture firm's FOMO. For example, in March 2021, BlockFi raised $350 million at a valuation of $3 billion co-led by Bain Capital Ventures, partners of DST Global, Pomp Investments and Tiger Global. The bankruptcies rattled the market. However, crypto was able to find its equilibrium again — in part thanks to the centralized currency exchange FTX which pledged to make further investments in infrastructure, including to buy the assets of Voyager Digital for $1.4 billion.

The UIgly… Highlighted by the spectacular collapse of the centralized crypto currency exchange, FTX — $32B valuation just days before the bankruptcy — appear to have [mis]used client's funds to prop up its highly speculative venture fund, Alameda Research, and other embattled crypto firms mentioned above. When the house of cards collapsed, the company's balance sheet appeared to show $9B of liability against $900MM of assets as reported by the Financial Times. Many of financial media (Bloomberg, Matt Levine; FT, Antoine Gara in New York and Kadhim Shubber and Joshua Oliver in London) have laid out the sequence of events in detail. To make matters worse, FTX seem to have suffered a cyberattack and $370MM of assets appear to be lost!

So, if we weigh the good, the bad and the ugly; a few points become clear.

First point, in a hyped and un-regulated market, such as crypto, *investor* knowledge and education are key. In this article, I focus on closing the knowledge gap – far from exhaustive – in the crypto market by examining the technology stack, the ecosystem and the risks.

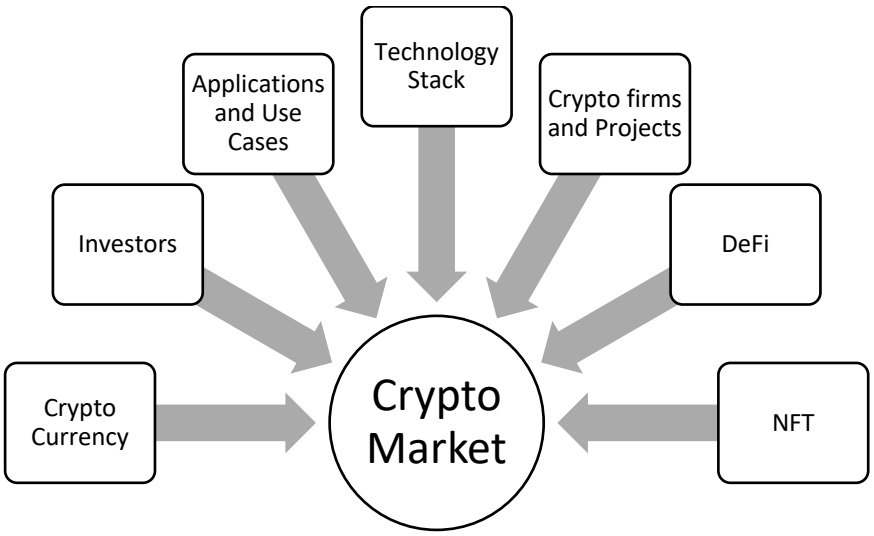
Second observation…is that for now, the crypto market and traditional financial markets are reasonably separated (Annie Lowrey, The Atlantic) limiting the risks to traditional financial

markets. However, as investment portfolios are diversified into the crypto world, the line between crypto and traditional finance will blur and the separation will evaporate.

…And the third key point is the failure of big-time investors in doing proper due diligence in their crypto investments, with a few notable exceptions that saw FTX as a complete risk and didn't participate in the investment frenzy. According to the MarketWatch, in the 2021 high, the crypto market valuation was ~$3T (yes, with a T!). As of this writing, valuation is at $850B, a historical loss of capital, and it is not over yet. Regular investors – individuals, participants in funds, pension fund contributors, etc. – however, relied on the big-time investors. This is a major lesson for doing your own due diligence and a motivation for you to read on…

What is the Crypto Market?

Crypto market is an extensive ecosystem consisting of technologies, products and projects, and investors as shown in the diagram below.



Assembly of figure by M. Mahdavi

From an *investor centric* point of view, an overlay of *transparency*, *governance, operations*, and *risk management* and *ease of use* should be integrated in every aspect of the crypto market.

Investors can play in the crypto market in several ways, some of the more popular channels are by participating in venture funds, buy crypto currencies on the crypto exchanges or invest in funds made up of basket of crypto currencies.

The crypto market is fraught with risks and potentially high returns albeit, the crypto billionaires! Besides the hype, risk and volatility, the crypto market, due to its infancy, exposes the investors to high levels of technical innerworkings causing further *opaqueness* and confusion. We will

focus on demystifying the crypto for the regular investor by introducing the main concepts, market dynamics and some of the risks.

What is Crypto Currency?

There are over 20,000 cryptocurrencies listed on CoinMarketCap (as of August 2022). Cryptocurrency is an electronic medium, designed to be used over the internet, that allows peer-to-peer transfer of value without the need for authority from third parties. Indeed, the decentralized nature of cryptocurrencies is one of its distinctive features that has brought many investors and interested parties to the crypto world. Bitcoin, which was launched in 2008, was the first cryptocurrency, and it remains by far the most influential and best-known. Over time, Bitcoin and other cryptocurrencies like Ethereum have grown as digital alternatives to money issued by governments.

Crypto currencies promise certain unique features:

- Cryptocurrencies make it possible to transfer value online without the need for a middleman like a bank or payment processor, allowing value to transfer globally, near-instantly, 24/7, for lower fees.
- Cryptocurrencies are usually not issued or controlled by any government or other central authority. They're managed by peer-to-peer networks of computers running free, open-source software. Generally, anyone who wants to participate is able to.
- If a bank or government isn't involved, how is crypto secure? It's secure because all transactions are vetted by the blockchain. Blockchain is a breakthrough technology only recently made possible through decades of computer science and mathematical innovations. We will discuss blockchain in the follow-on sections.
- Cryptocurrencies allow individuals to take control over their assets

There are two main types of crypto currencies: *crypto coin and crypto token*. While the two terms are often used interchangeably, they are not the same.

> Key Point
>
> *Crypto coins* are digital currencies designed to work within a particular blockchain and function like fiat currency in that they store value and are a means of exchange between two parties.
>
> *Crypto tokens* are digital assets, coded within smart contracts, created by the decentralized applications (dApps) and platforms built on top of an existing blockchain.
>
> Bitcoin, for example, is a coin and not a token.

Crypto coin is a cryptocurrency that is native to the blockchain it runs on. Because you cannot create a coin without building a blockchain, it is not easy to launch a coin. A prime example of a coin is Bitcoin, or BTC which is powered by its own blockchain with the same name. As BTC was the first established cryptocurrency, coins which appeared afterwards are called altcoins — alternative coins. All altcoins have their own standalone, independent networks as well. Top cryptocurrencies which qualify as coins (according to Coingecko) are Bitcoin, Ethereum, and BNB. Crypto coins have three common characteristics: They have their own dedicated blockchain, they act as money, and they can be mined (via POW or POS which we will discuss in a later section).

Crypto token is a digital unit of value that represents an asset or utility. Unlike coins, tokens do not have their own blockchain and are issued on top of existing networks. Unlike coins, tokens are not mined in the process of transaction validation. Instead, they are minted. Tokens can be used to raise funds or to give access to particular services. Another popular type of crypto token is the stablecoin, which is a token that follows the price of the U.S. dollar.

Tokens can be classified into three types:

- Security token – is a digital tokenized form of a traditional security. Security token holders do not have any ownership rights to the entity which issued the tokens. The tokens are sold through a public offering called a security token offering (STO). Just like traditional securities, security tokens are regulated by bodies such as the U.S. Securities and Exchange Commission (SEC).

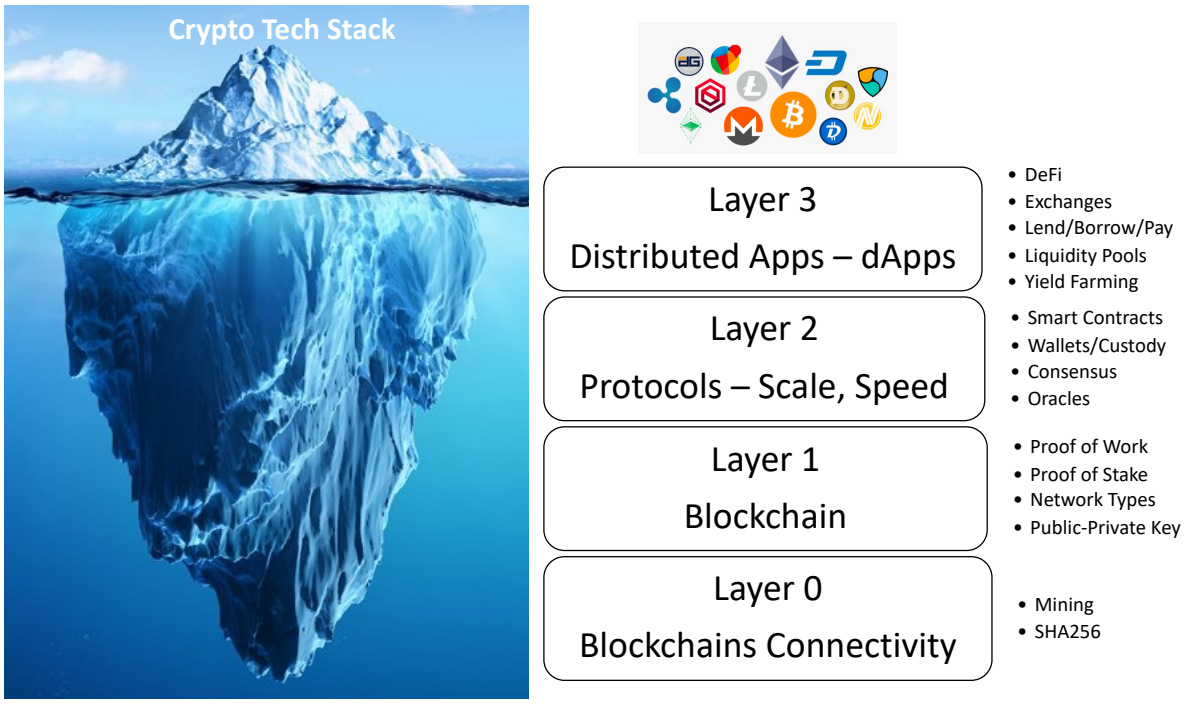
- Equity token – function like traditional stock assets and provide ownership to the token holders. Investors are entitled to a share of the company's profits and right to vote on decisions. Equity tokens are issued through an equity token offering (ETO) process.

- Utility token – provide access to an application or services of a blockchain-based project. Some utility tokens also offer discounts, rewards, and other benefits to token holders. Utility tokens are commonly issued through an initial coin offering (ICO).

> Key Point
>
> **Cryptocurrencies use a technology called public-private key cryptography** to transfer coin ownership on a secure and distributed ledger (blockchain). A *private key* is a secure password that is never needs shared with anyone, including those you send value on the network. A paired *public key* is shared with others to receive value on the network. With the public-private key cryptography, it is near impossible for anyone to guess your private key. The Public-Private Key management requires a complex infrastructure called *Public Key Infrastructure (PKI)*. This critical technology needs to properly be deployed and managed to ensure the security and privacy required in crypto transactions.

Crypto Technology Stack

Crypto currencies are supported by a stack of technologies that are organized into [architectural] layers as shown in the following figure:



Assembly of diagram by M. Mahdavi, inspired by @pastry

Each layer of technology stack provides specific services:

Layers 0 and 1– Blockchain and Connectivity

Layer 0 is the initial stage of blockchain infrastructure and allows for cross-chain interoperability such as Bitcoin, Ethereum, etc. Layer 1 of blockchain provides more advanced capabilities on top of layer 0. However, layer 1, also called the implementation layer, has scalability and speed limitations that are addressed in Layer 2.

Blockchain is the fundamental technology underpinning the crypto ecosystem**.** A cryptocurrency blockchain is similar to a bank's balance sheet or ledger. Each currency has its own blockchain, which is an ongoing, constantly re-verified record of every single transaction made using that currency. Unlike a bank's ledger, a cryptocurrency blockchain is distributed across participants of the digital currency's entire *network*. Each transaction is verified by participants in the network which is referred to as a *node* (sometimes called a miner).

Once the relevant participants (nodes) agree on the details of the transaction, that transaction is cryptographically encoded and packaged into a new *block* and the new block is broadcast to other nodes on the network. In the blockchain structure each block is connected to the block established before it, creating a *chain.* The security of the assets stored in each block are maintained cryptographically with the use of *Keys* and *Signatures.* By design, the resulting chain of blocks cannot be altered.

There are two types of Blockchain networks: *Permissionless and Permissioned*. In a permissionless network, anyone could join the network and allowed to contribute to it by adding transactions to the block by either providing Proof of Work (POW) or Proof of Stake (POS), which we will describe next.

Permissioned network restricts access to approved participants / trusted entities. In addition, certain participants may have different levels of access. A permissioned network allows for a centralized governance structure and enables assignment of responsibilities to a network operator. Decision-making may be more centralized for certain aspects of the network and more distributed for other aspects. The new generation of platforms managing lifecycle of security tokens, can handle both permissionless and permissioned networks for the settlement of a transaction.

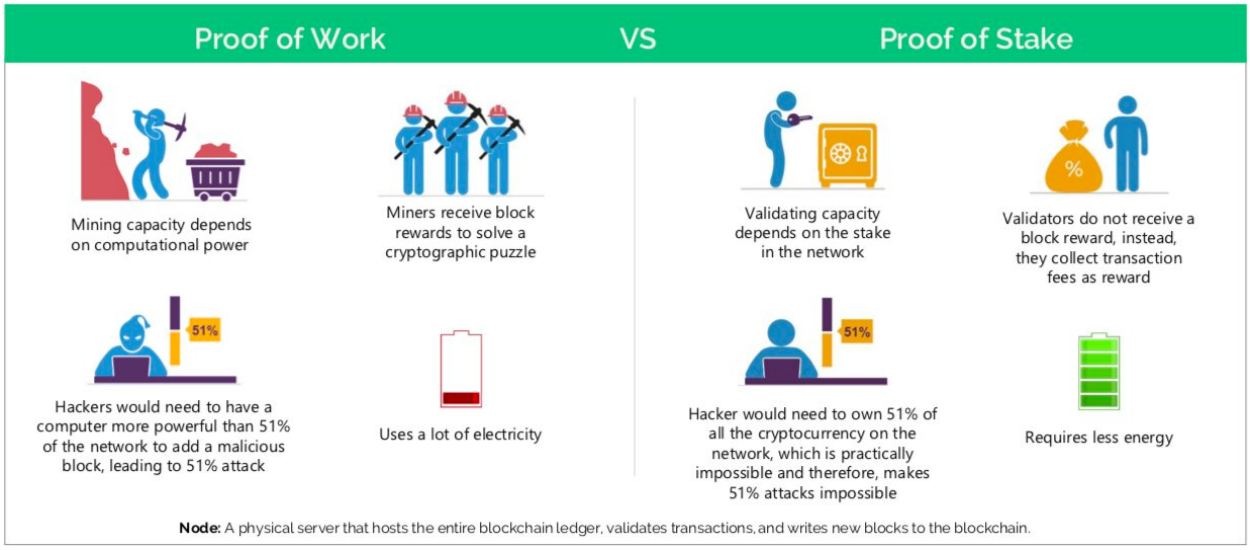
Permissionless network, such as Bitcoin or Ethereum, require Proof of Work (POW) or Proof of Stake (POS) to validate, add or maintain transactions. In return, network participants get rewards in the form of coins or a percentage of the transaction fees.

Proof of Work (PoW) is a mechanism that requires members of a network, sometimes called *miners*, to solve an arbitrary mathematical puzzle to gain the right to verify transactions and add blocks to the blockchain. PoW is a computationally intensive protocol that underpins the Bitcoin blockchain and many other cryptocurrencies (crypto coins). Miners engage in a competition to solve a mathematical puzzle on the PoW system to verify transactions. A reward in the form of cryptocurrencies is awarded to the miner who successfully adds to the blockchain block.

Proof of Stake (POS) addresses the computation and power requirements of POW. The POS method requires participant confirm transactions by staking coins rather than through competitive mining. Other mechanisms for becoming a participant in the network include Delegated proof of stake (DPoS), proof of authority (PoA) and proof of burn (PoB).

> Key Point
>
> In order to join and contribute to a (permissionless) blockchain network, participants are required to provide **Proof of Work (POW) or Proof of Stake (POS)**. In the PoW method, miners engage in a competition to solve a mathematical puzzle. POW is computationally intensive. Proof of stake (PoS) mechanism requires participants to stake their crypto to become a validator in the network. Validators are responsible for the same thing as miners in Proof of Work

The process and rewards for POW VS POS are shown in the figures below.



Credit: @pastry

Layer 2 – Scale and Speed Protocols

Layer 2 of crypto technology stack addresses the scalability and speed of blockchain transactions.

Consensus is a fundamental process for the operation of blockchain. Since the nodes on the network, are distributed and may be located in any part of the world, the *consensus* mechanism provides the protocols for agreement on actions that will take place on the blockchain network. A consensus mechanism provides a system for nodes on a computer network to agree on the validity of transactions to help secure that network. The two most common consensus mechanisms are proof of work (PoW) and proof of stake (PoS).

> Key Point
>
> **Consensus** mechanism is a fault-tolerant automated process to reach an agreement on a single state of the network among distributed nodes. These are protocols that make sure all nodes are synchronized with each other & agree on transactions, which are then added to the blockchain.
>
> **Governance** is generally accomplished through consensus. As a result, no single legal entity is responsible for governance decisions, record keeping, or dispute resolution.

Governance in the permissionless networks, is accomplished through a *Decentralized Autonomous Organization (DAOs)* is tasked with the governance structure. DAO is an organization represented by rules encoded as a computer program that is transparent, controlled by the organizations members and not influenced by a central government. Because the identities of permissionless users and contributors are unknown, they have not been qualified through *Anti-Money Laundering (AML), Know-Your-Customer (KYC)* or other regulatory processes, unless the governance structure of the system allows for special nodes to have access rights for oversight and regulatory compliance.

> Key Point
>
> ***Governance*** of the blockchain network is implemented by a mechanism called **Decentralized Autonomous Organization (DAOs)** which is an organization implementing a protocol with the rules encoded as a computer program that is transparent, controlled by the DAO members and not influenced by a central government.

Smart Contracts is a significant feature of the blockchain which are self-executing code – programs that run when predetermined conditions are met – used to automate the execution of an agreement. For example, a smart contract could potentially set forth the automatic procedures and processes for executing a transaction. Regulators can watch contract activity for oversight while keeping the privacy of the individual network participants.

> Key Point
>
> ***Smart Contracts*** are computer codes that are integral to blockchain operations. The code, and the conditions in it, are publicly available through the ledger. When an event in the contract is triggered, like an expiration date or an asset target price is reached – the code executes. Regulators can watch contract activity in real time while maintaining the privacy of the individuals.

Wallets and Custody are key to the investor activities and transaction. A crypto wallet is a place where you can securely keep your crypto. There are many different types of crypto wallets, but the most popular ones are hosted wallets, non-custodial wallets, and hardware wallets. Which one is right for you depends on what you want to do with your crypto and what kind of safety net you want to have.

Hosted wallets are the most popular and easy-to-set-up. It's called hosted because a third party keeps your crypto for you, similar to how a bank keeps your money in a checking or savings

account. You may have heard of people “losing their keys” or “losing their USB wallet” but with a hosted wallet you don’t have to worry about any of that. The main benefit of keeping your crypto in a hosted wallet is if you forget your password, you won’t lose your crypto. A drawback to a hosted wallet is you can’t access everything crypto has to offer. With a hosted wallet, you can Buy or transfer crypto. Most crypto platforms and exchanges allow you to buy crypto using a bank account or credit card. If you already own crypto, you can also transfer it to your new hosted wallet for safe keeping.

Self-custody wallets provide complete control of crypto to the investor. Non-custodial wallets don’t rely on a third party — or a “custodian” — to keep your crypto safe. While they provide the software necessary to store your crypto, the responsibility of remembering and safeguarding your password falls entirely on you. If you lose or forget your password — often referred to as a “private key” or “seed phrase” — there’s no way to access your crypto. And if someone else discovers your private key, they’ll get full access to your assets. In addition to being in full control of the security of your crypto, you can also access more advanced crypto applications like *yield farming, staking, lending, borrowing,* and more.

Hardware wallets reside on a physical device, about the size of a thumb drive, that stores the private keys to your crypto offline, for example, they can keep your crypto secure even if your computer is hacked. Similar to a non-custodial wallet, a hardware wallet typically doesn’t allow you to buy crypto using traditional currencies (like US dollars or Euros), so you’ll need to transfer crypto to your wallet and hence creating a security vulnerability.

> ☼ Key Point
>
> ***Wallets and Custody*** are the most visible tools used by the investors. A crypto wallet is where you can securely keep your crypto. The most popular wallets and custody are **hosted wallets, non-custodial wallets, and hardware wallets.** Security, ease of use and range of activities are the main criteria for choosing the type of wallet and custody.

Oracles are entities that connect blockchains to external systems so that smart contracts can execute based on inputs and outputs from the real world. "Blockchain oracle" is a method of feeding information into a smart contract. However, an oracle must be a *trusted data source.* Oracles sometimes need to reconcile different sources of information and feed them into a smart contract. With only one chance to get things right on the immutable blockchain, users must have confidence in the reliability of the data.

Layer 3 – Decentralized Apps (dApps)

Layer 3 of blockchain is referred to as the "application layer". The main task of this layer is to host the distributed Apps (dApps) and other protocols that enable a wide range of applications from finance to pharma to supply chain industries.

A key new addition to blockchain apps is a suite of applications called the ***DeFi – Decentralized Finance***. DeFi is a global peer-to-peer (meaning directly between two people, not routed through a centralized system) service that can offer privacy of individuals and transparency of transactions.

DeFi Apps are built on top of the most popular DeFi protocols. *Protocol* is a technical term. You can think of protocols as the *common rules*, *standards or workflows* written for governing particular tasks, use cases, or activities. DeFi protocols can feature a collection of rules and business workflows in the real-world financial institutions.

DeFi takes the basic premise of Bitcoin — digital money — and expands on it with the goal to create digital alternative to the Wall Street without all the associated costs (like intermediaries, etc.). The promise of DeFi is to open the financial markets that are accessible to anyone with an internet connection (many people around world don't have a bank account).

DeFi apps – using popular protocols/services – provide a range of financial services such as:

- **Lending**: Lend out your crypto and earn interest and rewards
- **Getting a loan**: Obtain a loan instantly without filling in paperwork, including extremely short-term "flash loans" that traditional financial institutions don't offer.
- **Trading**: Make peer-to-peer trades of certain crypto assets — as if you could buy and sell stocks without any kind of brokerage.
- **Alternative investing:** Put some of your crypto into savings account alternatives and earn better interest rates than you'd typically get from a bank.
- **Buying derivatives**: Make long or short bets on certain assets. Think of these as the crypto version of stock options or futures contracts.

> Key Point
>
> **DeFi** ecosystem promises to create many "digital alternative" use cases that the Wall Street offers with the benefits including reduced costs for transactions (no intermediaries), transparency, and markets accessibility.

Investors typically engage with DeFi via software called dApps ("decentralized Apps"), most of which currently run on the Ethereum blockchain. Decentralized finance apps use smart contracts on a blockchain.

Figure below, shows the traditional financial services that could be morphed into a DeFi technology stack.

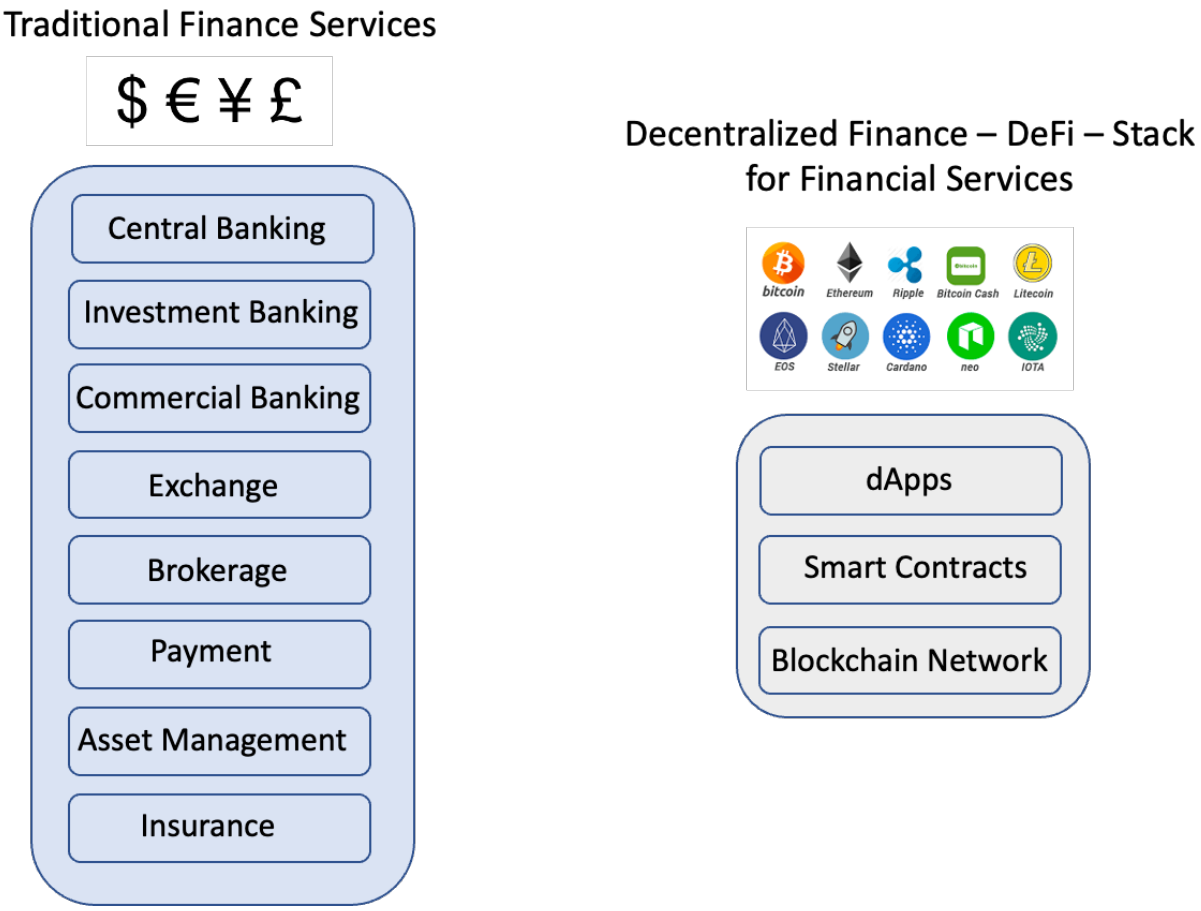


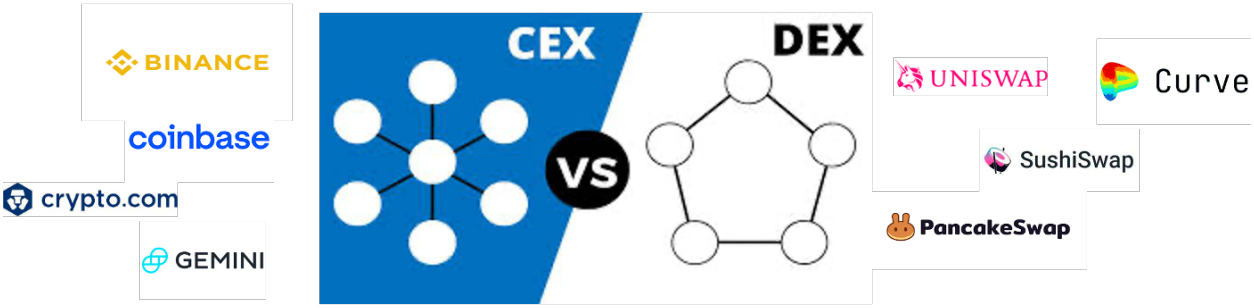
Figure assembled by M. Mahdavi

> Key Point
>
> Although, the crypto technology stack, through the DeFi apps, may make it possible to offer many traditional financial services, they provide there are business and operational processes that need to be in place for a working financial market. Regulations, oversight, risk management, governance, security controls, etc. need to be worked out on a global level before DeFi can become replacement for the Wall Street. However, certain applications of finance could become viable targets for the DeFi architecture. However, as of this writing, there are no "killer Apps" that would bring DeFi to the centerpiece of financial services.

Exchanges are the gateway for the investors to interact with the world of crypto. Exchanges connect several stakeholders together including buyers and seller of crypto instruments and the liquidity providers. Exchanges enable execution of the conditions coded in the smart contracts by providing several services such as: protocol governance, automated market making with pricing based on the total available liquidity across the trade pair, automated matching of buyer and seller orders.

There are two types of exchanges: **Central Exchanges (CEX's)** act as a trusted intermediary for the buying and selling of cryptocurrency with *custodial* function. In this model, the central exchange holds the investor's private keys. **Decentralized Exchanges (DEX's)** are a type of cryptocurrency exchange which allows for direct peer-to-peer cryptocurrency transactions to take place online with *non-custodial* function, meaning the user always remains in control of their private keys when transacting on a decentralized exchange.

You can buy cryptocurrencies on both centralized or decentralized exchanges. The figure below, shows the difference between the centralized VS decentralized exchanges and some of the providers for each exchange.



Assembly of the concepts and collage by M. Mahdavi

Decentralized apps (dApps) offer a wide range of financial services that are comparable to the traditional finance. Some of the main dApps are described in the following:

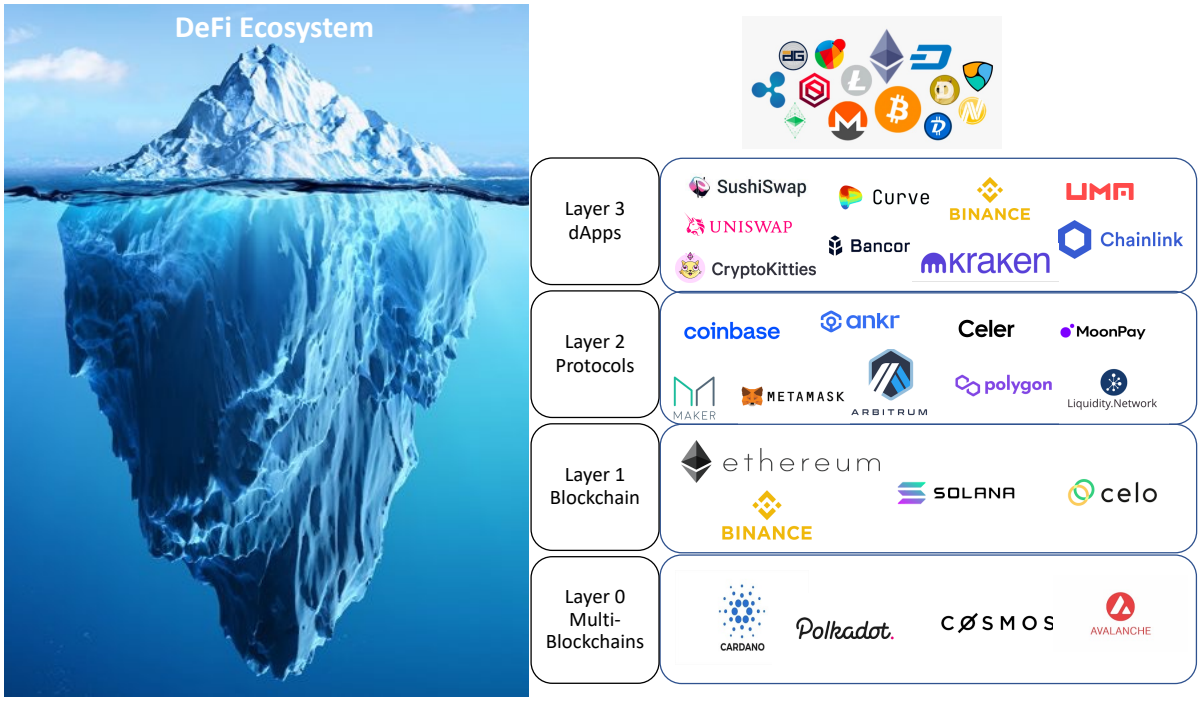
Liquidity Pool services is a crowdsourced pool of cryptocurrencies or tokens locked in a smart contract that facilitate trades on decentralized exchanges. Smart contracts automatically unlock transactions between parties once conditions are met. Several DeFi services (dApps), offer lending and trading through liquidity pools, where nobody acts as an intermediary for settling trades.

Yield Farming is the crypto equivalent of earning Annual Percentage Yield (APY) on deposits with banks. At its core, yield farming is a process in which liquidity providers lock up their assets in a liquidity pool and receive incentives in the form of trading fees or earning of tokens.

Lending/Borrowing of crypto is similar to the concept of traditional lending. Crypto lenders can lend out their idle assets to borrowers, who in turn pay out interest on the lender's assets.

DeFi Ecosystem

In the last few years, an extensive ecosystem of DeFi firms and projects have emerged enabling similar services as the traditional financial services. A representative example of projects for each layer of the technology stack are shown in the figure below.



Assembly of diagram by M. Mahdavi, inspired by @pastry

Today, there are several thousand projects in play globally that use DeFi applications. DeFi projects such as AML/KYC, legal and insurance are available and support the ecosystems.

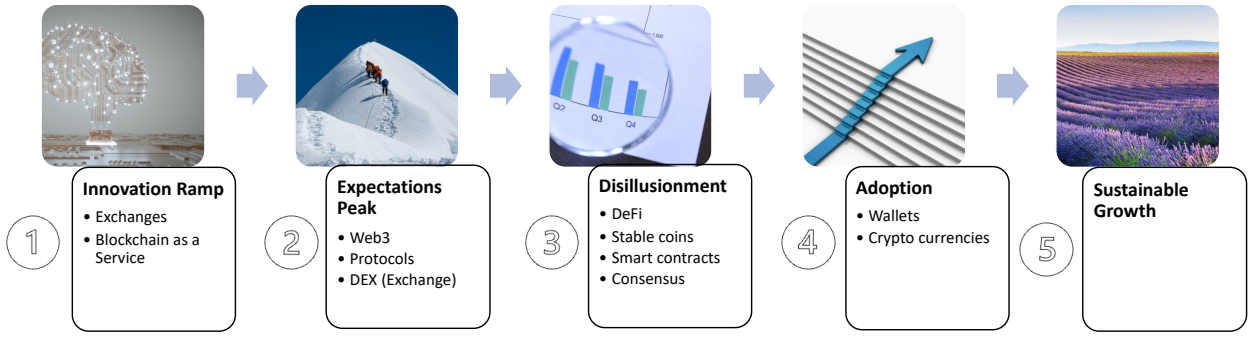
NFT and gaming is another ecosystem of its own implementing same technology stack as DeFi.

The underlying blockchain technology is also the fundamental layer of service for web3 which is the next generation of the internet, called the internet of value.

Enterprise applications ranging from aircraft maintenance to food safety, use tokenized real-world assets on top of the blockchain technology stack, to deliver business value in multiple industries.

The Crypto Stack Hype Cycle

Every new disruptive technology encounters the hype cycle, and the crypto stack and DeFi are not an exception. In the following, I propose the hype cycle for different components of the crypto technology stack based on the well-established technology hype curve by Gartner.



Adoption of the Gartner Hype Cycle for the crypto stack

Step 1 consists of technologies – such as centralized exchanges and blockchain as service – that are in the process of innovation and development.

Step 2 of the hype cycle involves technologies that have reached a high level of visibility and carry excitement and un-managed expectations.

Step 3 involves those technologies that are being deployed and are falling short of meeting the high expectations. This is mostly due to the nascent nature of the technology. It takes time for these technologies to mature.

Step 4 of the cycle involves technologies that have gone through the trial and errors of step 3 and growing on adoption. Wallets and crypto currencies are at this stage of the cycle since they have been deployed and growing in acceptance from a technical point of view.

Step 5 consists of the technologies that have gone through the ups and downs of the hype cycle and have reached a plateau of productivity per Gartner's definition. The Crypto stack is not at this stage yet.

> Key Point
>
> To provide *sustainable productivity and growth* for businesses and investors, all technology components of the crypto stack have to reach the step 5 of the hype curve. This stage for the crypto stack could be 2-5 years out according to the Gartner blockchain and web3 hype cycle.

Crypto Risk Assessment

Recent spectacular collapse of FTX and – to a lesser extent – other crypto providers such as Celsius, Blockfi, Voyager Digital, 3AC, and Genesis, highlight the risks of playing the crypto market.

The DeFi model, avoids the control of your funds by the exchanges with your cryptocurrency in your personal wallet, protected by your private key, and the smart contracts, ensuring automatic execution of the trading rules once the conditions are met. This is all good, however, in the DeFi ecosystem, the *counterparty risk* shifts over to *technology risk* including the management of the DeFi token in your wallet, management and safekeeping of your private key(s) in your wallet, and managing the danger of hacks, which are worryingly commonplace.

Another big problem in the current environment is that DeFi's growth since 2017 is correlated with *centralized crypto*, not as an alternative to it. In the case of Celsius Network and FTX, for example, we have seen how *centralized crypto* is a big borrower in DeFi pools, muddying the transparency benefits offered by DeFi.

The total value locked in DeFi tokens as of this writing is $43 billion, which is 74% less than the end of March 2022. On top of falling crypto token prices, there have been likely withdrawals.

> Key Point
>
> The lesson to learn from FTX's collapse isn't just that opacity is bad, but that all of crypto is an interconnected ecosystem in which assets are created without relation to real-world wealth and then used as collateral to further inflate what boils down to a single, enormous credit risk.

From an investor point of view, the main risks in the crypto market include:

- Cyber security and crypto key pair management (PKI),
- Volatility of cryptocurrencies,
- Hyped valuations,
- Governance and
- Regulations.

Cyber security risks refer to compromising the chain of devices and software that hold your private keys (and cryptos). There are many *attack vectors* against which your system needs to be protected. Techniques and methods for protecting the system storing your keys (and cryptos) are

outside of the scope of this work. However, due diligence in ensuring cyber security of your keys is essential.

Public Private Key Infrastructure (PKI) is directly related to generating and managing your private keys. The PKI systems is most likely provided by the crypto firm or the chain of service providers supporting the firm and its crypto offering. Audit of the PKI system by your Exchange or your Fund Manager should be available for your review.

To manage volatility risks, several tools and metrics are available. Ratings based on criteria such as liquidity, security, technology, governance, business operations, etc. are available by several external service providers.

Going forward, investor's due diligence – specially related to crypto exchanges and fund managers – will be critical. For example, exchange ratings are available through several providers.

> Key Point
> Due diligence and follow-on risk management are key for investing in the crypto market. Due diligence criteria should include governance, business operations and practices, liquidity (in real time), cyber security controls, PKI audit, and technology stack.
>
> It is noteworthy to consider the statement from the new CEO of FTX, John Ray III: "I have never seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information."

Regulations are in the state of flux as of this writing. DeFi is a global service and therefore many countries and jurisdictions are involved. There are several regulatory initiatives are underway around the world. In the US, current regulatory efforts include the case of SEC VS Ripple Lab's XRP token which can bring a level of clarity to the crypto market one way or another. The extent and projection of any regulations is outside of the scope of this work. However, lack of clarity, represent a major risk for the investors.

Use Case – Equity Tokenization with Blockchain

There are several applications that are being rolled out in scale such as central clearing and settlement of securities (in traditional finance transactions) by The Depository Trust & Clearing Corporation (DTCC) (working with R3 Corda) and Broadridge (working with VMware and Digital Asset DAML) that prove the value of crypto technology stack for mainstream financial institutions, totally independent of cryptocurrency and NFT trading.

The Depository Trust & Clearing Corp. (DTCC) – processing basically every trade in the more than $40 trillion U.S. stock market – just recently announced that it began live testing of a

private blockchain to see whether it's up to the challenge of clearing and settling transactions in the world's largest equities market. The Project Ion platform now processes more than 100,000 trades per day on average, and almost 160,000 on peak days. Although, this is a small number of transactions compared to the daily volume in billions of shares, it represent a milestone in traditional finance's efforts in embracing the ledger technology underpinning bitcoin (BTC) and the rest of the cryptocurrency ecosystem. Settling stock trades in the U.S. currently takes two days, which is a glacial pace compared with capabilities in the digital age. During feverish trading of meme stocks early last year, Robinhood restricted trades in some of them because of a $3 billion collateral request from DTCC, which stockpiles money as a safeguard in case something bad happens during the two days it's processing a trade. Major Wall Street players have for years been experimenting with blockchains. The former president of the New York Stock Exchange told the Wall Street Journal in a story that "blockchain technology is going to rewire all financial services."

The U.S. Securities and Exchange Commission (SEC) has proposed speeding up stock settlement times to something called T+0 – referring to processing trades the same day they're executed.

The DTCC project, which is private and permissioned unlike many permissionless blockchain networks such as Bitcoin and Ethereum, is being developed with firms including Barclays (BCS), BNY Mellon (BK), Charles Schwab (SCHW), Citadel Securities, Citigroup (C) and Credit Suisse (CS).

The Takeaways:

In investigating The Good, The Bad and The Ugly in the crypto market, the first and foremost takeaway is the investor education. The market is un-regulated and riddled with techno language and terms specific to crypto. In this article, we attempted to provide an investor centric review of the technology stack, definitions, the players and the potential risks.

As part of The Good, technology stack is burgeoning with innovation, but there is a hype curve…and technologies such the smart contracts, Defi and crypto wallets are on a 2-5 year development horizon. It is key to understand the crypto technologies and their ecosystem to perform your due diligence and invest accordingly.

Due diligence is key in everything crypto. Lack of due diligence has also led to unusually high valuations creating the bubble in the cryptocurrencies comparable to the dotcom bubble. This bubble is working through the system as at the time of this writing.

Corporate governance and operational oversight of crypto firms have proven to be critical in light of this nascent market.

Regulations are in flux and complicated develop. Regulations would make more sense iof they are use case dependent and how they fit into the financial system.

In the short term, investors should focus on their own due diligence before and during the lifecycle of their investment.