

STAKE HODLER CAPITALISM

Blockchain and DeFi
(Decentralized Finance)



AMR WAHBA METWALY

Stake Hodler Capitalism: Blockchain and DeFi (Decentralized Finance)

Table of Contents

[Stake Hodler Capitalism: Blockchain and DeFi \(Decentralized Finance\)](#)

[Disclaimer](#)

[Introduction](#)

[Author's Note](#)

[Chapter 1: DeFi Apps: The Ultimate Killer Apps in Blockchain](#)

[What Is DeFi?](#)

[Cryptography](#)

[Chapter 2: Blockchain](#)

[Storage structure](#)

[Decentralization](#)

[Transparency](#)

[How secure is blockchain?](#)

[Bitcoin vs. Blockchain](#)

[Ways Blockchains Are Implemented](#)

[Banking and finance](#)

[Currency](#)

[Health care](#)

[Records of property](#)

[Supply chains](#)

[Pros and Cons of Blockchain](#)

[Blockchain Advantages](#)

[Disadvantages of Blockchain](#)

[Chapter 3: Introduction to Smart Contracts](#)

[The Operation Process of a Smart Contract](#)

[How can you use smart contracts?](#)

[Government](#)

[Management](#)

[Automobile](#)

[Real estate](#)

[Healthcare](#)

[Benefits of Smart Contracts](#)

[Problems of Smart Contracts](#)

[Chapter 4: Ethereum and DeFi](#)

[Popular DeFi Apps: Lending and borrowing](#)

[MakerDAO](#)

[DAI Overview](#)

[Stable-coin](#)

[With Cryptocurrency](#)

[Decentralized Exchange](#)

[Degrees of Decentralization](#)

[Compound](#)

[Derivatives](#)

[DAOs](#)

[Prediction markets](#)

[Saving](#)

[Staking](#)

[Tokenization](#)

[Trading](#)

[DeFi vs. CeFi](#)

[Differences between DeFi and Open Banking](#)

[Why the Hype?](#)

[Benefits of DeFi](#)

[Advantages of DeFi](#)

[DeFi and Potential Risks](#)

[Chapter 5: What Does Yield Farming In Decentralized Finance \(DeFi\) Mean?](#)

[Don't You Need A Lot of Money To Run A Bank?](#)

[What Do Pools Mean?](#)

[Yield Farming: Overview](#)

[What is TVL \(Total Value Locked\)?](#)

[How Yield Farming Occurs](#)

[How Is The Profitability Estimated In Yield Farming?](#)

[DeFi and Collateral Deposits](#)

[The Dangers Inherent In Yield Farming](#)

[Crypto Yield Farming Platform and Protocols](#)

[Compound finance \(COMP\)](#)

[MakerDAO](#)

[Synthetix](#)

[Aave](#)

[Uniswap](#)

[Curve Finance](#)

[Yield Farming of Curve Bitcoin](#)

[Balancer](#)

[Balancer liquidity mining](#)

[Yearn finance](#)

[Chapter 6: Ways to Mine Your Bitcoin on Your Own](#)

[Get a wallet](#)

[Join a pool](#)

[Get a miner](#)

Keep your mind on the prize – your money

Conclusion

Disclaimer

Copyright © 2021

All Rights Reserved.

This e-book contains material protected under International and Federal Copyright Laws and Treaties. This e-book is intended for personal use only. Any unauthorized reprint or use of this material is prohibited. No part of this book may be used in any commercial manner without the author's express permission.

Scholarly use of quotations must have proper attribution to the published work. This work may not be deconstructed, reverse engineered, or reproduced in any other format. The entire e-book in its original form may not be shared with other users who don't obtain proper access to it.

Introduction

Entering into the blockchain ecosystem can seem a little bit hard and confusing for anyone, regardless of their background. Most people lose out on what blockchain technology and cryptocurrency as a whole offer because it's hard to identify ambiguous opportunities. The terminologies look a bit too technical and confusing. However, blockchain is a disruptive technology that looks promising and enticing to enthusiasts of decentralization and efficiency.

This book explains technical concepts in the simplest human-readable format. You will get to understand the key fundamentals of blockchain technology. By the end of this book, you will have sufficient knowledge of blockchain and DeFi that helps you identify strengths, weaknesses, opportunities, and threats.

Author's Note

This book series is one of the masterpieces I'm most proud of. I attribute this success to god, first and foremost, my mother and wife, family, and friends. A big part of what shaped me as the person I am now is when my dad passed away in 2018, which left me wondering about life's real purpose. At that point, I realized that the joy comes from the journey and the most rewarding feeling comes from helping other people.

Blockchain has had its fair share of disruption in our lives since Oct. 31st, 2008, which is the date Satoshi Nakamoto the creator of bitcoin, published his paper titled "A Peer-to-Peer Electronic Cash System." Nevertheless, bitcoin has had its direct effect on my life. I started delving into blockchain in 2017 when I got the idea of researching a blockchain-related ecosystem project; that was when I fell in love with blockchain and DeFi. In the "Stake Hodler Capitalism" book series, we will delve deeper into why I and many others have been fascinated to the point of obsession with Blockchain, cryptocurrencies, and decentralized finance.

Chapter 1: DeFi Apps: The Ultimate Killer Apps in Blockchain

Whether you have heard about the DeFi (Decentralized Finance) hype or you haven't heard about it, it already started being directly a part of our day-to-day lives. Throughout this chapter, we will break the components of DeFi into smaller, easily digestible subparts.

What Is DeFi?

DeFi or decentralized finance is a movement started by different researchers to create a new and open-source financial system that anyone can access without requiring trusted intermediaries or central authorities such as banks, brokerages, or exchanges. Cryptocurrencies are known to operate on a blockchain or public ledger technology implemented specifically as the backbone for it; the advantages offered by each of these smaller ecosystems

formed by cryptocurrencies are unimaginable. Bitcoin (although many currently consider it a store of value similar to gold) is still the first, most known, and best example. Payments can be made through the Bitcoin network, i.e., a network of decentralized independent nodes to confirm transactions.

To achieve this, DeFi relies heavily on cryptography, blockchains, and smart contracts. Before referring to this whole idea as decentralized finance, it was referred to as "open finance." A smart contract is the main building block of DeFi. On DeFi platforms, most people are permitted to lend or borrow funds from others, guess on changes in price on a couple of assets using derivatives, trade cryptocurrencies, insure against risks, and go ahead to make interest in a savings-like account. DeFi applications provide high risk-reward ratios, but joining some of these projects can be high risk in itself. Vetting out the best projects is a cumbersome process, but understanding the fundamentals will help you make the best investment decisions for Blockchain and DeFi.

Cryptocurrencies are known to operate similarly to the traditional banking systems we have. When it comes to payments, we can achieve the same results with blockchain. The killer edge that blockchain has over conventional banking systems is the immutable and decentralized nature. Decentralization can give you a hundred percent uptime versus what traditional payment systems offer nowadays. The immutability of blockchains guarantees the elimination of fraud. Bitcoin (although many now consider it a store of value like gold) is still the first and best example. Alice can pay Bob in Bitcoin without relying on a financial intermediary like banks. Instead, payments can be made through the Bitcoin network, i.e., a network of decentralized independent nodes to confirm transactions.

To recap, for all of this to occur, DeFi relies heavily on cryptography, blockchain, and smart contracts. Don't worry if you don't know what a smart contract is or how it simply functions. We will go over Smart Contracts in Chapter 3 of this book. If you want more deep dive into Smart Contracts, you can check out Part 2 of this book series titled: "Stake Hodler Capitalism: Smart Contracts and DApps."

Cryptography

Encryption is considered to be the core component of cryptography. More generally, encryption is creating and analyzing a protocol that prevents third parties or the public from reading or accessing data stored or transferred through a communication medium. The human-readable format for the DeDefinition of encryption is a BlackBox that you enter a piece of data to and use a key to encode it, and this process can't be reversed except with a unique key that two or more parties can share.

At the heart of modern encryption are various aspects of information security such as data confidentiality, integrity, authenticity, and non-denial. Modern cryptography is at the intersection of mathematics, computer science, electrical engineering, communications, and physics. Cryptographic applications include e-commerce, chip-based debit cards, digital currencies, computer cryptography, and military communications.

Before modern times, cryptography was almost synonymous with cryptography that turns knowledge from readable to unreadable nonsense. Encrypted message transmitters use decoders only for their intended recipients, making them inaccessible to attackers. The names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("Block") for the attacker are often used in cryptographic literature. Since the development of rotary encryption machines during World War I and the advent of computers during World War II, encryption technology has become more complex, and its applications have become more diverse.

Modern cryptography is primarily based on mathematical theory and computer science practice. Cryptographic algorithms are designed based on assumptions about computer security, making it difficult for attackers to exploit such algorithms. It is theoretically impossible to hack a well-designed system like this, but in practice, it is possible with quantum computers, but that is a topic beyond the scope of this book. For now, let's think of the use of cryptography as the safest way to store and deliver data. Hence, these circuits are called "data safe" if they are well designed.

Due to theoretical advances such as improvements in integer decomposition algorithms and faster computational techniques, these designs must be constantly reviewed and corrected if necessary. Although theoretically, it is impossible to break secure circuits even with unlimited computing power, such as one-time buttons, these circuits are theoretically the best broken but

much more difficult to use in practice than safe circuit computers.

The advancement of encryption technology has raised many legal and privacy issues in the information age. Due to cryptography's potential to be used in espionage, illicit activities, and other counterfeit applications, many governments have classified it as a weapon and have restricted or even banned its use and export. Skype, for example, uses a proprietary custom implementation of the AES (Advanced Encryption Standard) encryption algorithm. If you don't know what AES means, the important thing to understand is that cryptography is what keeps our privacy and safety assured during this information age.

Some jurisdictions where the use of encryption is legal may require legislators to disclose encryption keys for documents related to investigations. Encryption also plays an important role in digital rights management and copyright infringement disputes over digital media. Information and law enforcement agencies have long been interested in encryption. Confidential communications can be criminal or fraudulent. As a result, there is a history of conflicting legal issues with encryption, especially with the advent of low-cost computers making high-quality encryption more widely available.

In some countries, even the internal use of encryption is restricted. Until 1999, France severely restricted cryptography within its borders but later abolished many rules. Encryption licenses are still required in China and Iran. Many countries have strict restrictions on the use of encryption, especially in creating communication channels.

Although encryption is legal for home use in the United States, there have been many conflicts over legal issues related to encryption. One of the most important issues was the export of encryption software and tools. Perhaps because of the importance of cryptography during World War II and the expectation that cryptography will continue to be important to national security.

After World War II, it was illegal to sell or distribute cryptographic technology abroad in the United States. Encryption was designated as additional military equipment and placed on the U.S. Army list. Before the

advent of PCs, asymmetric key algorithms (e.g., public key methods), and the Internet, this wasn't that much an issue. However, as the internet grows and internet-capable computing devices become more accessible, high-quality encryption methods have become known worldwide.

Chapter 2: Blockchain

Blockchain is a special kind of database. It differs from a typical database when it comes to storing information. Blockchain stores data in blocks that are interlinked. It collects information in groups (also known as blocks) that contain sets of information. Blocks have a certain storage capacity, and when filled, they bind to previously filled blocks to form a data chain called a "blockchain." All new information after the newly added block is collected in the new blocks and added to the chain when filled, and the process continues indefinitely.

Blockchain looks complex in its formal DeFinition, but let's breakdown the concept into simple human-readable language. Blockchain is a chain of small links that are interconnected. Each link contains information, whether confirmed transactions between two parties or other data (e.g., Smart Contracts, Videos, Music, or any other form of data).

To understand blockchain, you first need to understand what a database is. A database is a collection of information electronically stored on a computer system. The information or data in a database is usually organized in tabular format to find and filter specific information easily. What's the difference between someone using a spreadsheet rather than a database to store information?

The spreadsheet is designed for small users or groups who can store and access a limited amount of information. However, databases are designed to store much more information that can be quickly and easily accessed, filtered, and manipulated by many users at the same time.

Large databases achieve this by hosting data on powerful computer servers. Sometimes, these servers can be built with hundreds or thousands of computers to provide the processing power and memory required for multiple

users to access the database simultaneously with the most efficient required access time. While many people have access to spreadsheets or databases, they are often owned by designated people who have full control over their work and the work within it.

When new data enters the blockchain, it is inserted into a new block. When a block is filled with data, it is pinned to the previous block, and the data is linked in chronological order. Different types of data can be stored on the blockchain, but the most common use has been the transaction ledger in Bitcoin and other cryptocurrencies.

When it comes to Bitcoin, the blockchain is used in a decentralized way so that no person or group has control, but instead, all users maintain control. Decentralized blockchains are tamperproof; therefore, this means that the recorded information is irreversible. For Bitcoin, this means that everyone is constantly visually registering transactions.

The critical aspect that most people fail to understand is how do these blocks get appended to the blockchain. The answer to that is through mining. In the simplest words possible, Mining is verifying the legitimacy of a block before it gets appended to the blockchain. That process is done by participating nodes that electively (In the case of bitcoin) choose to do so, and in return, they get a block reward. We will cover more on mining in Chapter 6.

Now that we are clear with the definition of concepts, you might find yourself asking, but what differentiates blockchain from a database? The following are a few of the differences:

Storage structure

A distinct difference between the usual database and a blockchain is how the data is structured. A blockchain compiles data or information together in groups, also known as blocks, which carry information sets. Blocks have specific storage capabilities, and when full, are bound onto the formerly filled block, going ahead to establish a chain of data called the "blockchain." All this new information that comes after the newly added block is stored into a freshly formed block which will then also be added to the chain once they get filled.

While a database structures its data into tables, a blockchain, like its name, connotes structures its data into blocks later chained together. Hence, all blockchains can be referred to as databases, but not all databases can be called blockchains. This system also naturally makes an irreversible timeline of data when enforced in a decentralized nature.

The moment a block is filled, it is set in some and automatically becomes a part of this timeline. Every single block in the chain is provided a precise timestamp when it becomes a part of the chain.

[Decentralization](#)

Same as a database, Bitcoin needs a compilation of computers to store its blockchain. For Bitcoin, blockchain is simply a type of database which houses every Bitcoin transaction which ever existed in a series of interlinked blocks. In the case of Bitcoin, and different from most databases, these computers do not all reside under a roof, and each computer or faction of computers is operated by a different individual or group of individuals.

Suppose a company has a server with about 10,000 computers with a database housing all of its client's account information. This company owns a warehouse containing all of these computers underneath a roof and has total control of and access to each of these computers and all the information each of them contains. Likewise, Bitcoin consists of thousands of computers; however, individual computers or pools of computers house its blockchain. These computers reside in different geographical locations, and they are all run by different people or groups of people. These computers that Bitcoin's network is known as nodes.

In this criterion, Bitcoin's blockchain is used in a decentralized manner. However, private and centralized blockchains where the computers form their network are owned and controlled by a sole being. These private blockchains can be implemented to fit your business needs and give you the advantages of blockchain while minimizing your data exposure to the public. Examples of platforms that offer private blockchain solutions are IBM Blockchain, Azure Blockchain, and AWS (Amazon Web Services) Blockchain solutions.

In the blockchain, every node has a complete history of the blockchain's data since its birth. For Bitcoin, the data is the full history of all Bitcoin

transactions. If there is an error in one node's data, it can use the thousands of other nodes as a reference to correct itself. This way, a single node within the network will not change any information held in it. Hence, the history of transactions in every block that encompasses Bitcoin's blockchain is not changeable.

If one user interferes with Bitcoin's record of transactions, all the remaining nodes would easily cross-reference and specify the node with the incorrect information. This system aids in building an accurate and transparent order of events. For Bitcoin, this information is like a list of transactions; however, it is probably for a blockchain to store different legal contracts, state identities, or a company's product inventory. A couple of the decentralized network's computing power would need to concur on the stated changes to make something else out of how the system functions or the information housed. This makes sure that any changes that happen are in the best interests of most, if not all, of them.

Transparency

Due to Bitcoin's blockchain being decentralized in nature, all exchanges can be transparently seen as either owning a personal node or using blockchain explorers, which permits anyone to see exchanges happening live. Every node has its unique copy of the chain that gets refreshed as new blocks are verified when added. Thus, if you want to, you are capable of tracking Bitcoin wherever it goes. For instance, cryptocurrency exchanges that have been hacked in the past and those who held Bitcoin on the exchange lost everything. Although the hacker may be unknown, yet the Bitcoins that they took away can easily be traced. Therefore, if the Bitcoins stolen in these hacks were moved or spent elsewhere, the original owner will be able to track them. There is also a concept called tainting coins, and it's the same as tainting money that gets stolen from banks through some form of colors.

How secure is blockchain?

Blockchain technology considers the matter of security and trust in different ways. First, recent blocks are always housed in a straight line and sequentially. They are always added to the "rear" of the blockchain. If you take a proper look at Bitcoin's blockchain, you will notice that every block has a place on the chain, and this is called a "height." Also, the block's height

has reached about 656,197 blocks so far.

The moment a block has been included at the end of the blockchain, it becomes pretty difficult to reverse and change the block's contents unless most users agree to proceed with the action. This is because every block is made up of its hash that looks something like this

0000001393nd5n3v32d134d214n14m02018, in addition to the hash of the block before it. What are hash codes? Hash codes are built by a math function that turns digital information into a sequence of numbers and letters that can be interpreted when inserted back into that function through specific means. If that information is altered in any way, the hash code will eventually change as well. This is quite a big deal to security.

Suppose a hacker wants to change the blockchain and illegally take Bitcoin from everyone else on the platform. If the hacker were to change their copy, it would no longer connect with the other people's copy. Therefore, when every user comes together to cross-check their copies against each other, they would notice that one copy seems different, and the hacker's version of the chain would be classified as not authorized.

For the hacker to succeed with such a hack, they would need to control and change 51% of the blockchain's copies one after the other, so the new copy of the community becomes the majority copy, leading to the consensus the claim. For such an attack to be a success, it will require a huge amount of money and resources because there is a need to redo all of the blocks from the beginning to the end as there will be different hash codes and timestamps following the alteration.

The size and fast growth of Bitcoin's network and the cost to pull off such a deal would be likely enormous. It would be expensive and infeasible, and also as destructive as the use of nuclear weapons. Going ahead with the hack will not go unnoticed by other users in the same community as they would see serious changes to the blockchain. The network members will then have to move on to a new part of the chain that has not been corrupted.

This would make the attacked part of the Bitcoin drop in value, and the attack would eventually turn pointless because the villain actor has gained control of nothing but a worthless investment. The same thing would happen again if

the hacker were to attack the new version of Bitcoin. It is designed this way so that being a part of the network is more economically encouraged than attacking it.

Bitcoin vs. Blockchain

The objective of blockchain is to enable digital information to be recorded and shared but not altered. Blockchain technology was initially mentioned in 1991 by Stuart Haber and W. Scott Stornetta; two researchers wanted to install a system where document timestamps are tamper-proof. However, it was not until two decades later that blockchain experienced its first real-world application' Bitcoin' was launched in January.

The Bitcoin policy was designed on a blockchain. In a research paper announcing the digital currency, Bitcoin's pseudonymous founder, Satoshi Nakamoto, referred to it as "a new electronic cash system that's entirely user-to-user," with no intermediaries trusted or not.

The crucial factor to comprehend here is that Blockchain's sole purpose isn't Bitcoin, to record a ledger of payments; however, in theory, blockchain can be used to make records of any number of data points rigidly. This could be in the form of regular monetary transactions, votes in an election, product inventories, state identifications, deeds to homes, etc.

Presently, there is a broad variety of blockchain-based projects looking to carry out blockchain to help society rather than just recording transactions. A good instance is that of blockchain being used as a way to vote in democratic elections. The nature of blockchain's immutability means that illegal voting would become a bit more difficult to happen.

For instance, a voting system could work such that each citizen of a country would be given a single cryptocurrency or token. Every candidate would then be presented with a particular wallet address, and the voters would send their token or cryptocurrency to whichever candidate's address they desire to vote for. The traceable and transparent nature of blockchain would dispel the need for human vote counting and hackers' ability to interfere with physical ballots.

Ways Blockchains Are Implemented

Blocks on Bitcoin's blockchain house data about the monetary exchange. However, it turns out that blockchain is a dependable way of keeping data about other types of transactions.

Some companies that have already included blockchain are Walmart, Pfizer, AIG, Siemens, Unilever, and many more. For instance, IBM has designed its Food Trust blockchain to trail food products' journey to get to its specific geography.

Why is this necessary? The food industry has witnessed countless outbreaks of E. coli, salmonella, listeria, and toxic materials being mistakenly introduced to foods. Previously it has taken weeks to discover the core of these outbreaks or the cause of sickness from the things people are eating.

With blockchain, brands are given the capability to track a food product's route from its source through each stop it makes and its final destination. The food can be trailed back through each stop to its source if a food is contaminated. Furthermore, these companies can also witness other things they may have come in contact with, identifying the problem that is likely to happen far sooner, thereby saving lives. We will cover more of Blockchain and IoT applications in part 3 of "Stake Hodler Capitalism: Blockchain and IoT (Internet of Things)."

This is an instance of the blockchains in practice, but there are many other blockchain implementation forms. Let's delve deeper into more applications of Blockchain.

Banking and finance

Maybe no industry stands a chance to gain from integrating blockchain into its business operations more than banking. Financial institutions can only operate during business hours, five days a week; this means that if you try to pay a check on Friday at 6 p.m., you will have to hold on until Monday morning to see that money get into your account. Even if your deposit is made during business hours, you may still need to wait one to three days to verify the transaction because of the large volume of transactions that banks need to settle. On the other hand, blockchain never sleeps or rests. Here, inside the blockchain ecosystem, every minute, all days of the week is a

business hour.

By changing blockchain into banks, consumers can now see their transactions processed in as little as 10 minutes. Banks also have the privilege to trade funds between institutions more rapidly and safely with blockchain. For instance, the settlement and clearing process can take up to three days - or longer if trading globally, in the stock trading business. This means that the money and shares are inaccessible for that duration. And with the help of Smart Contracts, these fully autonomous financial systems can be governed by a set of preDefined rules and regulations coded into these smart contracts. More on Smart Contracts in Chapter 3.

Regarding the sums involved, even the few days the money is in motion comes with crucial costs and banks' risks. Hence, European bank Santander and its research partners put the likely savings at \$15 billion to \$20 billion a year. Capgemini, a French consultancy, roughly calculates that consumers could save up to \$16 billion in banking and insurance fees every year with the aid of blockchain-based applications.

Currency

Blockchain shapes the foundation for cryptocurrencies like Bitcoin. The Federal Reserve controls the U.S. dollar. From this central authority system, a user's data and currency are basically at the mercy of their bank or government. If a user's bank is hacked, then the client's personal information is in danger. If the client's bank ceases to function anymore or they live in a country with an erratic government, their currency's value may be at risk. In 2008, some of the banks that were out of money were released using taxpayer money. These are the worries which conceived the birth of the famous Bitcoin.

By distributing its functions across a network of nodes, blockchain gives Bitcoin and other cryptocurrencies the ability to function without the need for a central authority. This does not only minimize risk but also takes away lots of processing and transfer fees. Those in countries with erratic currencies or financial infrastructures can also be provided with a more fixed currency with more applications and a vast network of users and institutions where business and transactions can be done both home and abroad. Nevertheless, cryptocurrencies have faced much opposition, with some claiming that it's a

replacement for the dollar. Still, if we think about it more carefully, we will find that the idea of a U.S. Crypto Dollar as a backbone for smaller ecosystems that have their tokens and cryptocurrencies is very attainable. Let's set aside the fears of quantum computing hindering cryptography, which is the backbone of encryption; such attacks are infeasible and can be mitigated with hard forks. On top of those mentioned above, the decision to launch a blockchain attack on a cryptocurrency owned by a government is the same as using nuclear weapons.

With cryptocurrency, wallets for savings accounts or as a means of payment are especially intense for those who have no state identification. While some countries may be war-torn, others have governments that don't have any real development to give identification. Citizens of such countries may not have an entry to savings or brokerage accounts and will have no way to store wealth safely.

Health care

Health care providers can utilize the blockchain to keep the medical records of their patients safely. The moment a medical record is created and signed, it can be written into the blockchain, and this leaves patients with the proof and boldness that the record cannot be tampered with. These private health records could be encoded and housed on the blockchain with a private passcode so that they are only available to specific individuals, hence making sure privacy is preserved.

Records of property

The process of documenting property rights is both stressful and lengthy; you will agree with this if you have ever spent time in your local Recorder's Office or other concerned government entities. Nowadays, physical documentation must be taken to a government employee at the local recording office, and then it will be manually inputted into the county's central database and public index. If there is a property dispute, the property's claims must be settled with the public index.

However, this process is not just expensive and time-wasting; it is also infested with human error, where every inaccuracy on the recorders makes tracking property ownership nearly impossible. Blockchain can destroy the

need for looking through documents and trailing down physical files in a local recording office. If property ownership is housed and confirmed on the blockchain, owners can rest assured that their title is correct and forever recorded.

Also, it can be almost impossible to show ownership of a property in war-torn countries or areas with little to no government or financial infrastructure, especially the absence of a "Recorder's Office." If several people living in such an area can use blockchain, transparency and distinct property owners' timelines could be founded.

Supply chains

Suppliers can make use of blockchain to store the origins of materials that they have bought. This would allow companies to cross-check the genuineness of their products, in addition to some common labels like "Organic," "Local," and "Fair Trade." According to Forbes, blockchain's use to trail the way to ensure food safety all through the farm-to-consumer voyage.

Pros and Cons of Blockchain

For its entire complicated manner, blockchain's possibility as a decentralized form of record-keeping is almost without restrictions. Ranging from greater user privacy and increased security to reduced processing fees and little errors, blockchain technology may as well view applications far more than those mentioned above. However, there are also some disadvantages.

Pros

- Improved correctness by taking away human participation in verification.
- Reduces costs by taking away the intermediary verification.
- Decentralization makes it difficult to meddle with and also ensures a hundred percent uptime.
- Transactions are safe, personal, and productive.
- Transparent technology.
- It provides a banking choice and way to safeguard private information for citizens of countries with erratic or undervalued democracies.

Cons

- Significant energy consumption and pollution from mining.
- Low TPS (Transactions Per Second) when compared to VISA and other systems.
- A long history of illicit activities utilizing cryptocurrencies that are based on Blockchain.
- Absence of regulations and formal regulatory bodies.

Blockchain Advantages

Accuracy of the chain

A network of thousands of computers (node) verifies all transactions on this network. This eradicates almost all human participation in the verification process, leading to a reduced amount of human error and a correct information record. Should a computer on the network make an inputting mistake, the error would only reflect a copy of the blockchain. Before the error can spread to the rest of the blockchain, it would require to be made by at least 51%, which is a majority of the network's computers—which is likely impossible for a large and growing network as of Bitcoin's.

Efficient transaction settlement time

It can take a few days for transactions put through a central authority to be settled. For instance, if you try to deposit a check on Friday evening, the funds may not reflect in your account until Monday morning. While financial institutions function during business hours - five days a week, blockchain works 24/7 yearlong without a break. Transactions can be finished in as little as ten minutes and can be considered safe after just a few hours.

Private transactions

Many blockchain networks function as public databases; this means that anyone with a strong internet connection can see a list of the network's transaction history. Although users can check details about transactions made, they can pinpoint information about the users making those transactions. It is common to think that blockchain networks like Bitcoin are anonymous and confidential, and secure.

This means that when a user makes an exchange in public, their one-of-a-kind code called a [public key](#) is documented on the blockchain instead of their personal information. If a person has purchased Bitcoin on an exchange that needs identification, then the person's identity is still connected to their blockchain address, but a transaction, even when tied to a person's name, does not expose any personal information.

Disadvantages of Blockchain

Although there are major gains to the blockchain, there are also major challenges to adopting this. The difficulties or obstacles to the application of blockchain are not just technicalities. The true challenges are political and regulatory mostly, not to mention the thousands of hours of custom software design and invisible programming needed to incorporate blockchain to present business networks. Here are some of these challenges:

Technology cost

Although blockchain existence saves users money on transaction fees, the technology is not entirely free. The "proof of work" algorithm and system that Bitcoin uses to verify transactions digest huge amounts of computational power. In the physical world, the millions of computers on the Bitcoin network are almost equal to what Denmark consumes every year.

Regardless of the costs of mining Bitcoin, users still increase their electricity bills to approve transactions on the blockchain. When miners include a block to the Bitcoin blockchain, they are gifted with enough Bitcoin to make their time and energy count. For blockchains that do not use cryptocurrency, miners would like to be paid or otherwise encouraged to verify transactions.

Certain solutions to these issues are starting to arise. For instance, Bitcoin mining farms have been set up to use solar power, excess natural gas from fracking sites, or wind farms' power. That would help face the drop in block rewards as we get near mining all the 21 million bitcoins in existence.

Speed inefficiency

Bitcoin is the best example of the potential inefficiencies of blockchain. Bitcoin's PoW (proof of work) system takes about ten minutes to include a new blockchain block. At that speed, it's calculated that the blockchain network can only take care of about seven transactions per second (TPS). Although other cryptocurrencies such as Ethereum function better than Bitcoin, they are still restricted by blockchain. Legacy Visa systems, for context, can process up to 24,000 TPS.

Solutions to this problem have been in development for years. Currently, some blockchains are bragging over 30,000 transactions per second.

Illegal activities

On the blockchain network, users are protected from hacks and preserves privacy. However, it also gives a chance for illegal trading and activity on the blockchain network. The most cited instance of blockchain being used for illicit transactions is probably the [Silk Road](#), an online “dark web” drug marketplace operated from February 2011 until October 2013 when the FBI shut it down.

The website gave users access to browse the website without being trailed using the Tor browser and making illegal purchases in Bitcoin or other cryptocurrencies. The present U.S. rules need financial service providers to get information about their customers when they register an account, examine each customer's identity, and make sure that customers do not appear on any list of suspected or current terrorist groups. This can have both its curses and blessings, mainly because it grants anyone access to financial accounts and allows criminals to carry through with their exchange. People have argued that the good uses of crypto, like banking the unbanked world, outweigh the bad uses of cryptocurrency, especially when many illegal activities are still done via untraceable cash and fiat currencies.

Chapter 3: Introduction to Smart Contracts

“Smart contracts...guarantee a very, very specific set of outcomes. There’s never any confusion, and there’s never any need for litigation”. – Jeff Garzik, owner of blockchain services Bloq

Smart Contracts are simply programs that run on the Ethereum blockchain. It is a set of code (functions) and data (states) located at a certain Ethereum blockchain address. Smart contracts are a form of an Ethereum account. What it implies is that it contains a fund balance and can activate transactions across the network. Nonetheless, it cannot be controlled by a network member. Instead, it is programmed and distributed across the network and works as pre-set or pre-coded. User accounts can interact with smart contracts by sending transactions that perform functions DeFined in the smart contract. Smart contracts specify rules as regular contracts, and these get enforced automatically using code.

Smart contracts assist with the exchange of money, property, shares, or anything valuable in a transparent, non-conflict way while forgoing the services of a middleman. Specific output is guaranteed with the correct input. This logic is coded in the vending machine the same way it is coded into a smart contract.

Anyone can sign smart contracts and use them on the web. All that is required of you is to learn to code in smart contract language and have enough ETH to use the contract. Using a smart contract is technically a transaction, so you have to pay for gas in the same way you pay for a simple ETH transfer. However, the gas cost of using the contract is much higher.

Ethereum provides a coder-friendly language for writing smart contracts Called “Solidity.”

- Solidity

Solidity is an object-oriented coding language for writing smart contracts. The great thing about Ethereum is that smart contracts can be programmed in a relatively developer-friendly language. If you have experience with Python or JavaScript, you can find a smart contract framework to use with a familiar syntax.

Smart contracts regulate the behavior of accounts in the Ethereum platform. Solidity is inspired by C++, Python, and JavaScript and is structured for the Ethereum Virtual Machines. It is mainly used to perform smart contracts on various blockchain platforms such as Ethereum. It was developed by Christian Reitwissner, Alex Beregsazi, and several former Ethereum key contributors to enter smart contracts on blockchain platforms. The Solidity programming language is primarily intended for code development and implementation of the Ethereum virtual machine.

Furthermore, smart contracts establish the rules and penalties surrounding an agreement in the same way that a conventional contract does, but it also enforces those obligations automatically.

- Vyper

Vyper allows you to program on Ethereum, a blockchain-based virtual machine that permits smart contracts' design and execution without the need for centralized or trusted intermediaries. It was developed to improve after Solidity, another smart contract language for Ethereum, by restricting unsafe practices and increasing readability. Vyper finds to run the security and audits of smart contracts efficiently.

Vyper is an experimental, contract programming language just like python and statically written. Like objects in the OOP, every contract has state variables, functions, and similar data types. Contract-particular characteristics are event notifies listeners, custom global variables, and global constants.

Some Ethereum contract instances are crowdfunding, voting, and blind auctions, to mention but a few. Nonetheless, it must be compiled before use so that the Ethereum VM can deduce and store the contract. Smart contracts are publicly available on Ethereum and can be considered an open API. This means that other smart contracts can call their smart contracts to expand their functionality greatly. Contracts may also activate other contracts.

By itself, smart contracts cannot send HTTP requests and therefore cannot accept "actual" event information. This is intentional because the use of external information can undermine the consensus important to security and decentralization.

The Operation Process of a Smart Contract

The smart contract is an automated computer code for executing all or part of a contract. It is commonly saved on a platform that is built on the blockchain. Such a code may only represent a contract between the parties, or it may be used to support a standard textual contract and comply with specific provisions, like the transfer of funds from one party to the other.

The multiple blockchain nodes can thus benefit from the blockchain's durability, security, and immutable nature. This mockup equally implies that the code essentially executes when a fresh block is integrated into blocks or blockchain chains. At the beginning of the transaction, if the participating persons indicate that certain parameters are fulfilled, the code automatically performs the action initiated by these parameters.

The code will only do this when a transaction is initiated. When there is no such transaction, the code will do nothing until such a time a transaction is initiated or activated. Most smart contracts are coded using a coding language close in syntax to many widely used programming languages for computer programs like Solidity.

Presently, the factors and the approval measurements of smart contracts must be specified. It also needs to be set as objective goals. What this means is things like, if "A" happens, follow step "B." So, a smart contract's actual work is a very basic task, like routinely transferring some cryptocurrencies from a single party's wallet to another's wallet based on certain criteria. As the blockchain grows and streamlines or the number of assets transferred to the chain increases, smart contracts will get more sophisticated and handle complex transactions. More on Smart Contracts' applications will be covered in "Stake Hodler Capitalism: Smart Contracts and DApps."

Developers already combine several steps in the transaction process to create more advanced smart contracts. However, it will take at least a few years for the code to define more subjective legal standards, like the party's compliance with reasonable commercial operating standards or the need for compensation and compensation provisions. There are many law firms hiring developers so they can participate in the new era of contractual agreements.

Before smart contracts are implemented on any blockchain, another essential thing required is to pay the contracts' execution fees. For instance, if a smart contract is to be executed in the Ethereum blockchain, the contract procedures are commonly performed on the Ethereum Virtual Machine (EVM), and the parties to the contract pay for the transaction using the Ethereum crypto coin called "gas" or ether. The more complicated a smart contract is, depending on the transaction stages, the higher the amount of gas you have to pay to fulfill the smart contract. Therefore, gas is currently an important gateway to avoiding EVM congestion with overly complex or multiple smart contracts.

Presently, Smart contracts are great for routinely carrying out two types of "transactions." The first one is ensuring that money is paid for certain triggers, and the second one is to impose sanctions on financial terms if specific laid down contract terms are not fulfilled. In each of these two instances, once smart contracts are deployed, and work begins, no human intervention or a judiciary intervention is necessary. This minimizes the operational and execution cost of the contract system.

For instance, smart contracts can remove the need for the operational holes known as procure-to-pay. If a consignment reaches a warehouse and goes through the required scanning process, the smart contract immediately launches the application for the necessary authorization and, upon receipt, can instantly transfer money from the buyer to the seller.

The seller will receive their payments faster, and there wouldn't be any need for dunning, and the buyer will minimize the cost of payment. This can affect the need for working capital and streamline financial transactions for the two transacting parties. Once enforced, smart contracts can be encoded to disable access to an internet-based asset if payment is not received. For instance, accessing specific content may be automatically withdrawn if no payment is made.

According to Vitalik Buterin, a 27-year-old programmer of Ethereum, he explained the smart contract in this way. In a smart contract system, an asset or a currency is transferred into a program which then executes this code, and at some point, it automatically validates a condition and determines if the asset should go to person X or back to person Y, or if it should be instantly

reimbursed to the person who sent it or some mixture of both.

The decentralized ledger also keeps and duplicates the document, which permits it a certain security and immutability. For example, if you rent an apartment from someone, you can do this via the blockchain by making payments in cryptocurrency. Then, you will get a receipt held in your virtual contract with your landlord, who in return gives you the digital entry key that comes to you on a particular date. Suppose the key does not come in on time; the blockchain will release a refund. However, if the key is sent before the rental date, the function will keep it stored, thereby releasing both the key and fee to you and your landlord respectively when the specified date comes.

The system functions on the If-then premise and is often witnessed by hundreds of people, so you can rest assured to expect a flawless delivery. If your landlord gives you the key, then he is sure to be paid. If you send several amounts in Bitcoins, you will receive the key. The document is instantly canceled after the time, and the code cannot be disturbed or touched without the knowledge of both of you since all participants are always notified of whatever exchange goes on. You can utilize smart contracts for any situation ranging from financial derivatives, contract breaches, financial services, insurance premiums, property law, credit enforcement, legal procedures to crowdfunding agreements.

How can you use smart contracts?

According to Jerry Cuomo, the Vice President for blockchain technologies at IBM, smart contracts can be used across all areas ranging from financial services, health care, insurance, etc. Here are ways through which smart contracts can be utilized:

Government

With smart contracts, citizens no longer have to worry about their votes being rigged because it will calm all concerns by producing a long-lasting, tamperproof and secure system. Ledger-protected votes would need to be decoded and needs a lot of computing power to gain access to it. Since no one can possess that much computing power as is directed to it, it would need the godlike computing power to hack or infiltrate the system.

Also, smart contracts could pull low voter turnout up. Many inactivities

originate from an imbalanced system that includes queuing, showing your identity, and filling out forms. Volunteers can even transfer voting online, and a thousand will turn out as a group to vote for their leaders.

Management

Not only is a single ledger provided as a source of trust by the blockchain, but probable complications in communication and workflow are also due to its accuracy, transparency, and automated system. Usually, business operations have to adapt to and fro while patiently waiting for the approvals after the internal and external bodies are finished sorting themselves. A blockchain ledger optimizes this, and it also cuts out any issues that may naturally happen with the independent procedure, which may lead to expensive lawsuits and delays in settlements.

Automobile

There is no argument that we are moving forward from the lazy pre-human vertebrates we were to the extremely smart robots. If we think of a future where all things are automated, we will realize that we are almost there with the existence of smartphones, smart glasses, and even smart cars. This aspect is where smart contracts can be of help. For instance, let us use the self-autonomous or self-parking vehicles as a case study. In this aspect, smart contracts can put in place an oracle of some sort that can tell whose fault it was in a crash; the driver, the sensor, or other parts in the vehicle.

With the aid of smart contracts, an automobile insurance company could authorize prices differently based on where and in what conditions customers are operating their automobiles. More on Smart Contracts applications in the second part of the series “Stake Hodler Capitalism: Smart Contracts and DApps.”

Real estate

More money can be made through smart contracts. On a norm, you would need to pay an intermediary such as an agent or a newspaper to advertise and then pay again so that you can confirm if the person has paid the rent and followed through with the remaining process, this is for someone who wants to rent out their apartment.

With smart contracts, the ledger reduces your costs. All you have to do is pay

with Bitcoin and encode your contract on the ledger. Everyone can see what you have done, and you achieve instant fulfillment. Brokers, realtors, hard money lenders, and others connected with the property game get to make a profit.

Healthcare

Personal health records can be encoded and classified on the blockchain with a private key that would give entry to only specific individuals selected beforehand. The same method can be used to ensure that research is performed through HIPAA laws securely and confidentially.

Furthermore, receipts of surgeries can be stored on a blockchain and automatically sent to insurance providers as evidence of delivery. The ledger can also be used for general healthcare management like overseeing drugs, regulating obedience, testing results, and organizing healthcare rations.

Benefits of Smart Contracts

Smart contracts are a key edge for Ethereum and other cryptocurrency ecosystems over ordinary fiat currencies. Here are some of the things that can be gotten or gained from using smart contracts:

Autonomy

Since you are the one agreeing, there is no need to depend on a broker, lawyer, or any other middleman for confirmation. Apropos also takes away the dangers of being manipulated by a third party. Since the job is automatically done by the network, instead of by one or more people, probably biased, or individuals that can make a mistake, your interest is secured.

Trust

Your data and files are encrypted on a shared ledger, so there is no way someone can say someone lost or misplaced them. You can always trust to find it whenever you need it.

Backup

It is possible for your bank lost your savings account. However, this is not the case on the blockchain, as you are in very good hands. Since every one of your friends got your back, your documents are duplicated many times over

and over.

Safety

You don't have to worry about security because your documents are safe with cryptography and websites' encryption. Hacking is not an option, and it would take an extremely craze and talented, smart hacker to crack the code and infiltrate your documents on this platform.

Speed

To manually process documents, you will have to spend lots of time and paperwork before accomplishing this feat. On the other hand, smart contracts use software code to automate assignments, therefore cutting hours off taking care of business processes or any other documented stuff.

Savings

Since the presence of an intermediary is taken away from the picture, smart contracts save you money by this exemption. For instance, you may have to pay a broker or notary to witness your exchange or help you monitor it.

Accuracy

Computerized contracts are known for their speed and cheapness and their ability to avoid the errors that come from filling out piles of forms. Here, errors are very much non-existent or extremely minimized.

Problems of Smart Contracts

“Smart Contracts are where the rubber meets the road for businesses and blockchain technology. While a few highly specialized distributed financial services use cases for blockchain have appeared—for example, payment ledger services for the Yangon Stock Exchange in Myanmar. Its services on top of the blockchain that is interesting. The Yangon Exchange solves distributed settlements in a trading system that only synchronizes trades twice a day. But the autonomous execution capacities of smart contracts extend the transactional security assurance of blockchain into situations where complex, evolving context transitions are required. And it's this possibility that has Amazon, Microsoft, Azure, and IBM Bluemux rolling out

Blockchain-as-a-service (Baas) from the cloud". – Patrick Hubbard, Head Greek, SolarWinds.

Smart contracts are far from perfect, even as wonderful and awesome as they sound. For instance, software defects can cause serious issues, the government can have a hard time regulating such contracts, the government may also have issues on ways to tax these smart contract transactions, there may also be the problem of sending the wrong code according to the rental example aforementioned or sending the right code, but your apartment gets condemned (I.e., made to become public use without your permission) before the arrival of the rental date.

Some of these things could be revoked in court, but the blockchain is a different issue. The contract proceeds no matter what happens until the stipulated end time. The challenges of smart contracts when the thought of goes on and on. Although experts are trying to correct them and make them perfect, these important issues discourage some likely users from hopping.

Blockchains where smart contracts processes can go through:

Bitcoin

Bitcoin is the perfect place for performing Bitcoin transactions; however, it has limited ability to process smart contracts.

Side Chains

This is another name for blockchains that run adjoining to Bitcoin, and they have a broader range to offer for processing contracts than that of Bitcoin.

NXT

NXT is a common blockchain forum that has a limited choice of templates for smart contracts. You have to use whatever resource you are given because you cannot code independently of these resources.

Ethereum

Ethereum is a known blockchain platform that is the most advanced for

coding and processing smart contracts. You are given the liberty to code whatever you desire but would have to pay for computing power with “ETH” tokens.

Smart contracts have no end to the number of industries they can influence from healthcare, real estate, and even the law. The list of its potentials goes on and on.

Chapter 4: Ethereum and DeFi

Let's start by specifying that presently, most if not pretty much all of the DeFi projects are built on Ethereum. Ethereum is a decentralized blockchain that allows other decentralized blockchain applications (dApps) to be built on smart contracts, and some of these apps can have their exchangeable tokens. The compound is one of the protocols that primarily deal with decentralized financial services that save and lend cryptocurrency.

The main reason for this is the fairly powerful Ethereum smart contract platforms that provide the robustness that allows you to write smart high-level contracts containing all the necessary logic for your DeFi application. Additionally, Ethereum has the most advanced ecosystem for all smart contract platforms. Thousands of developers create new applications every day, and the greatest value lies in smart contracts that create additional networking effects.

One of the widely adopted programming languages for smart contracts on Ethereum Blockchain is called Solidity. Solidity allows the creation of advanced smart contracts containing all the necessary logic for the DeFi applications. Besides, Ethereum has the most developed system amongst smart contract platforms, with an increasing number of developers building and creating new applications every day and the most value locked in a smart contract, creating an additional network effect.

This is perfect because Ethereum's platform for smart contracts gives more room for flexibility, and it instantly performs transactions if specific conditions are met. Ethereum smart contracts programming languages like Solidity are particularly created for developing and deploying such smart contracts. For example, if a user wants to send their money to a friend on a Thursday, only if the temperature skyrockets to 85 degrees Fahrenheit, according to weather.com. Another example would be changing your agricultural land rent prices based on corn futures (i.e., futures security) prices. Rules and clauses like this can be included in a smart contract. Lots of DeFi applications run on Ethereum with smart contracts at the center of them all.

Popular DeFi Apps: Lending and borrowing

MakerDAO

MakerDAO was one of the primary projects to take the first step in the DeFi movement. MakerDAO was founded in 2015 and allowed consumers to produce DAI, the world's first supported neutral currency and a leading decentralized stable coin. It also allows users to stake collateral to collect loans. DAI is a fixed coin that uses incentives to track prices in US dollars.

DAI can also be used to save money on the MakerDAO platform. It can be used for loans which is one of the pillars of the financial system. DeFi is trying to create a whole new economic ecosystem that doesn't require permission and is transparent. Borrowing and lending or staking is just part of this ecosystem. Other important features are fixed coins, decentralized exchanges, derivatives, margin trading, and insurance.

DAI is a stable crypto coin that tries to maintain its worth near the US dollar value (USD) using an automated smart contract system built on the Ethereum platform. DAI is sustained and operates under the governance structure of MakerDAO, which is a Dex Autonomous Organization (DAO) made up of MKR-controlled ticket holders who can vote on the alterations to specific parameters of smart contracts to keep DAI stable. The duo systems, DAI and MakerDAO, are regarded as the foremost and primary DeFi to gain massive attention and adoption.

As of June 2020, Compound Finance started compensating lenders and borrowers on its platform with units of a new cryptocurrency referred to as COMP token in addition to the normal interest payments to lenders. This COMP token is used to control Compound's platform but can also be traded on exchanges. Soon, other platforms followed the lead, thereby launching the prodigy known as 'yield farming' or 'liquidity mining.' COMP is a platform where observers shift cryptocurrency assets among different pools in a platform and among different platforms to increase their total yield, including interest and fees, but the value of additional tokens is collected prizes.

DAI Overview

DAI is based on overly secure security and redemption procedure enabled by MakerDAO smart contracts in the dApp form. Consumers who stake Ether

(or any other crypto coins supported as collateral) may obtain a loan worth the deposited amount and get the freshly created DAI. Currently, Ether's security ratio is set to 150%. This means that if you stake \$150 worth of Ether, you can obtain a loan up to 100 DAI (approximately \$100). If the collateral value falls below this percentage, the borrowed amount is routinely repaid through a smart contract. Conversely, if the cost increases, you can borrow extra DAI.

As a result, the returned DAI are automatically extinguished upon loan repayment and interest accrual, making it possible to withdraw the collateral. Thus, DAI's USD value is supported by the underlying collateral's USD value held by the smart contracts of MakerDAO.

Through the regulation of the supporting collateral, the terms of the collateral, and the borrowing or staking interest rate for MakerDAO's DAI can regulate the amount of DAI in circulation, which equally influences its overall value.

MKR token holders reserve the right to suggest and implement changes to these variables using the code. Governance token holders can vote on suggested changes, but the degree varies and depends on the number of tickets they hold. The MKR token is equally an investment tool in the MakerDAO platform. Along with the loan amount, the lender's additional interest is utilized to purchase and burn or finally withdraw the MKR tokens from the market. This procedure is intended to create MKR deflation to the degree that corresponds to the loaned amount. Let's talk about each one of the categories one by one besides MakerDAO that we just mentioned.

Stable-coin

Stable-coin is a cryptocurrency designed to reduce fixed-priced Bitcoins' volatility compared to "fixed" asset baskets or assets. Stable-coin can be linked to cryptocurrency, fiat currency, or commodities (e.g., precious or industrial metals). Soluble stables in currency, commodities, or fiat currency are known to be hedged, and the stables associated with the algorithm are called seigniorage (non-backed).

Stable-coins are cryptocurrencies linked to an asset outside of the cryptocurrency community, for instance, the dollar or euro. The main

objective here is to stabilize the price.

Backed Stable-coin

The advantage of asset-based cryptocurrency is that coins are stabilized by assets that fluctuate outside the cryptocurrency space. Since Bitcoin and Altcoins are highly correlated, cryptocurrency holders cannot avoid significant price declines without leaving the market or seeking refuge in an asset-based Stable-coin. Additionally, if these coins are managed in good faith and have an asset redemption mechanism, they are unlikely to be lower than the underlying physical asset's value due to arbitration.

Parallel stabilization is subject to the same volatility and risk as to the underlying asset. If fixed coins are protected in a decentralized way, they are relatively immune to predation, but having a central archive can lead to theft or trust loss.

Commodity Asset-backed

Stable-coin's main backup features:

- One or more items are worth and can be exchanged as needed (more or less).
- You have a promise to pay from an unregulated person, an open company, or a regulated financial institution.
- The number of goods used to maintain a fixed mooring must reflect the fixed supply's circulating supply.

Owners of commodities backed by fixed commodities can take over real assets by redeeming their shares at a conversion rate. The cost of maintaining Stable-coins stability is the cost of storing and protecting the underlying raw material. Take Digix Gold Tokens (DGX) and others as an example.

Fiat-backed

The value of this type of Stable-coin is based on the value of supported currencies in the hands of regulated third-party financial institutions. Confidence in the availability of treatment in this situation is very important to the stability of the price. Fiat-backed inserts can be traded on the stock exchange and redeemed from the issuer. Other key factors in Stable-coins stability are the cost of maintaining reserves and legal compliance, licensing required by regulators, and maintaining the auditors and business

infrastructure.

Cryptocurrencies supported by fiat currencies are the most common and were the first types of fixed coins to be released on the market.

Features of fiat-backed cryptocurrencies:

- Its value is fixed in one or more currencies (usually US dollars, euros, and Swiss francs) at a fixed rate.
- Communication takes place offline through banks or other regulated financial institutions that act as a repository of currencies used to support Stable-coins.
- The amount of currency used to support Stable-coin must be equal to the Stable-coin in circulation.

With Cryptocurrency

Cryptocurrency-based Stable-coins accept cryptocurrency as security and is conceptually similar to fiat-based Stable-coin. However, a key difference between the two interpretations is that while fiat collateral generally occurs outside the chain, the cryptocurrency used to support this type of Stable-coin blockchain is created using smart contracts decentralized approach. In most cases, it is more profitable to pay off the debt when the fixed value drops by blocking collateral so that consumers can borrow on smart transactions. To avoid sudden interruptions, you can cancel a consumer's loan with a smart contract if the collateral gets too close to the withdrawal amount.

The main features of Bitcoin backed cryptocurrency are:

- Bitcoin's fixed value is provided by another cryptocurrency or cryptocurrency portfolio.
- Binding is done on the chain through smart contracts.
- Fixed Bitcoin distribution is regulated within the chain through smart contracts.
- Achieve price stability by introducing additional means and incentives as well as collateral.

This type of filing coin's technical implementation is more complex and versatile than fiat-based filing lines, increasing the risk of exploitation due to the smart contract code's errors (bugs). Because models operate in chains, they are not subject to third-party regulations that create decentralized

solutions. A potentially problematic aspect of this type of Stable-coin is the change in underlying security value and hosting platforms. The complexity and indirect support of fixed coins can limit their use because it can be difficult to understand how the price is offered. Due to the highly volatile and highly convergent nature of the cryptocurrency market, very large collateral must also be maintained to ensure stability.

Decentralized Exchange

DEX (Decentralized Exchange) is one type of cryptocurrency exchange that enables direct peer-to-peer transactions with cryptocurrencies online, securely, and without intermediaries.

In transactions made through decentralized exchanges, the blockchain is usually replaced by the usual third-party organizations that monitor decentralized general ledgers' security and asset transfers (e.g., banks, securities brokers, online payment portals, authorities, etc.). Common work methods include using smart contracts or resubmitting orders, but many other options are possible and varying degrees of decentralization.

With the aid of online exchanges, users can exchange currencies for other currencies, be it in U.S. dollars for either Bitcoin or DAI. DEXs are the classy and hot exchanges that connect the users directly to ensure a promising trade on cryptocurrencies without dependence on an intermediary to work on their money.

Decentralized exchanges reduce the risk of stealing from hacked exchanges as consumers do not need to transfer their assets to the exchange. Advanced exchanges can also prevent price manipulation or counterfeit trading volumes through flushing and are more anonymous than active customer recognition. Know your customer (KYC) exchanges.

There are signs that decentralized exchanges are suffering from low trading volumes and market liquidity. Project 0x, a protocol for creating decentralized exchanges with funky liquidity, is trying to solve this problem.

Disadvantages

Since there is no Know your customer (KYC) process and the transaction is irreversible, you will lose users if they are hacked and their passwords or private keys are obtained. Although liquidity fund DEX is the most widely

used, it may have some drawbacks. The most common problems with DEX liquidity funds are price cuts and performance gains.

The decline in prices is due to the nature of Automated Market Makers (AMM). The larger the transaction, the more it affects the price. For example, if you use a consistent AMM product, all transactions must keep product $XY = k$ constant where x and y are the number of two cryptocurrencies (or tokens) in the pool. The larger the input size Δx , the lower the final y/x ratio, giving the exchange price. This issue is usually important for large companies or small liquidity pools.

A frontal launch is a special form of public block attack where participants (usually miners) proceed with their transactions (e.g., play with transaction fees) when they see an impending transaction, making the initial transaction less profitable.

Ideas for improving the tensile strength of permanent AMM products were first discussed in a post by Vitalik Buterin. One possible solution is to allow transactions that do not complete immediately but last for some time (e.g., 5 minutes), in which case the liquidity is gradually transferred to the pool without the highest price. This eliminates the problem of continuing travel because frontline workers cannot benefit from long work. It also helps prevent price slippage, as mediators and other traders can act in parallel, interfering with counter traders.

Degrees of Decentralization

Decentralized exchanges may still have a central component, which means that some control over the exchange remains in central institutions' hands. A good example is that IDEX prevents New York State users from placing orders on the platform.

In July 2018, it was reported that Bancor's decentralized stock exchange was hacked, causing \$13.5 million in asset loss before funds were frozen. Advanced exchange operators can obtain legal consequences from state supervisory authorities. An example is the founder of EtherDelta, who paid a fee with the US in November 2018. The Securities and Exchange Commission operates a privately held stock exchange.

Compound

There are a few other important DeFi products in this category. The main one is compound. Compound at the time of writing is the biggest DeFi project in the lending category, with around six hundred and thirty million dollars worth of assets locked in the protocol. The compound is an algorithmic autonomous interest rate protocol that allows users to supply assets like Ethereum or Tether and start making interest. Supplied assets can also act as collateral to enable their owners to borrow other assets.

User-to-user lending and borrowing policies are some of the most vastly used applications in the DeFi ecosystem. For instance, Compound utilizes an algorithm with autonomous interest rate protocol which combines with and underlies a long list of DeFi platforms such as PoolTogether, Dharma, and Argent.

By providing interest rate markets on Ethereum, Compound permits users to gain interest in crypto, which they have been supplied with to the lending pool. The Compound smart contracts automatically fit the borrowers and lenders, then calculate the interest rate based on the percentage of borrowed assets to supply investments. The compound is a clear example of the exponential opportunity of the DeFi domain. The more products are merged to the Compound policies, the more crypto investments will gain interest even when inactive.

The compound provides loans for certain cryptocurrencies such as Housing (DAI), Ether (ETH), USD Coin (USDC), Ox (ZRX), Tether (USDT), Wrapped BTC (WBTC), and Basic Featured Token (ATM), Augur (REP), and Sai (SAI). Any cryptocurrency owner or hodler can lend and borrow cryptocurrency directly without wasting time, effort, and money spent communicating with traditional financial intermediaries.

If you own the cryptocurrencies mentioned above, you can send, block, deposit, and borrow. They all mean the desired amount for the compound protocol. Locking cryptocurrency with Compound is the same as putting money in a savings account, but it uses a blockchain-based decentralized protocol. Instead of depositing money in the bank, they send cryptocurrencies to wallets. You start earning interest in cryptocurrency instantly, just like you're lending to a bank. The rate of return is indicated by the same symbol

as borrowed. In other words, sending BAT earns interest on BAT, and sending DAI earns DAI. The cryptocurrency you send is added to a huge fund from the same sign of The Compound Protocol's smart contracts sent by thousands of others worldwide.

On the other side of the equation is the loan. Blocking cryptocurrency in Compound allows you to get a loan on it. Some platforms do not require credit checks, so anyone in the world with cryptocurrency can apply for loans and get instant approval when the applicant meets certain conditions.

The compound is the quality of the assets that determine the amount you can borrow according to. For example, if you convert \$500 worth of Bitcoin to 1,000 COMPS and Compound has set Bitcoin's loan limit (also known as a security factor) to 50%, you can lend \$250 to other cryptocurrencies supported by the Compound protocol (see list top). Like when you borrow money from a bank, you have to pay interest on the money you borrow.

So we have deposits and loans, and both have to do with interest rates. When you stake, you earn interest. You pay interest on a loan you borrow. Let's talk about how these rates are automatically calculated and applied using a well-crafted system that is beautifully architected.

Whether you are borrowing or doing business, you must first exchange the cryptocurrency with Compound. This way, you will receive a complex token(s) (cTokens) representing your cryptocurrency balance in return. That token and many other tokens are created on Ethereum's blockchain as an ERC-20. ERC-20 tokens are one of the biggest advantages and innovations in the blockchain-based cryptocurrency market. When earning (or paying) interest, it can be transferred, sold, or programmed to other Dapps in the DeFi ecosystem just like any other Ethereum token. Treat these tokens as if they were managing digital assets on the Ethereum blockchain with public and private keys.

Interest rates depend on how much cryptocurrency (or liquidity) is available in each market and in real-time with supply and demand to reflect current market conditions. The interest rates displayed are listed as annual interest rates and are charged each time an Ethereum block is broken. Every 15 seconds, cToken's value increases by 1/2102400 (15-second blocks per year)

from the annual percentage quoted by Cryptopedia (n.d) at the time.

Another popular DeFi project is AAVE. Use smart contracts and specific incentives wisely. We can create Stable-coins linked to US dollars without having to store dollars in the real world. There are many other non-algorithmic dummy coins such as USDT, USDC, or PAC. The biggest problem is that they are centralized because they're backed by a company responsible for storing underlying equivalent assets being U.S. dollars or other assets.

However, Stable-coins have gained popularity and are often used as a compound or other in DeFi applications. Unlike central cryptocurrencies, decentralized exchanges or Dex allow cryptocurrencies to be exchanged in a completely decentralized and unauthorized manner without preventing coin storage. Examples of liquidity pools decentralized exchanges are Uniswap, Khyber, Balancer, and Bancor. Links and Idex are examples of book ordering systems.

Derivatives

Like traditional finance, derivatives are contracts whose value is determined by the return on the underlying asset. DeFi's main application in this space is Synthetix, a decentralized platform that provides access to various assets on the chain. Derivatives are products whose value is determined by the value of one or more variables called the base (the underlying asset). This base entity can be an asset, an index, or an interest rate and is often referred to only as "baseline." Derivatives can be used for various purposes, including insurance (hedge) against price movements, increased exposure to price movements to speculation, or access to difficult-to-trade assets or markets.

Ethereum-based smart contracts help create tokenized derivatives whose value is obtained from an underlying investment's success, through which partners' agreements are hardwired in code. DeFi derivatives can also indicate real-world investments like flat currencies, bonds, commodities, and even cryptocurrencies.

The most common financial derivatives include futures, options, swaps, and conversions such as synthetic collateral and credit swaps. Most derivatives are traded on OTC exchanges or exchanges such as the Chicago Mercantile

Exchange, while most insurance contracts are developed as a separate industry.

Derivatives are first on the list of main components of financial instruments; the other two are equities and liabilities (i.e., bonds and mortgages). Derivatives are contractual agreements between two or more parties that Define the terms to be paid between the parties (especially the date, amount, and Definition of the underlying variables, the parties' contractual obligations, and fictitious amounts).

Assets include stocks, commodities, bonds, interest rates, and currencies, but they can also be other derivatives, providing another tier that complicates accurate valuations.

Margin Trading

While margin traders in conventional finance can influence their trades by borrowing funds from a broker – that forms the collateral for a loan, DeFi margin trading, on the other hand, is powered by decentralized, non-custodial lending policies like Compound, Fulcrum, and dYdX. Due to conventional brokerage's smart contract automation, some have started to shift to the increasingly autonomous money markets' in the DeFi ecosystem.

Insurance

Insurance is another part of traditional finance that can be reproduced in decentralized finance. It provides a guarantee of compensation for payment of insurance premiums. One of the most widely used insurance applications in the DeFi space is for instances of smart contract error and deposit protection. The most popular DeFi projects in this area are Nexus, Mutual, and Opyn.

DeFi is still an upcoming domain with attendant risks surrounding smart contract bugs and breeches. Some creative insurance alternatives have come to the market to assist users with purchasing coverage to protect their holdings. Nexus Mutual is one of the solutions provided. It gives a Smart Contract Cover which safeguards against unintentional uses of the smart contract code.

Another very important but not very limited financial part of the DeFi

ecosystem is Oracle's services focused on delivering stable data streams outside of smart contracts. The most popular project in this area is chain link. These are found in almost every major part of the DeFi ecosystem. It can also be combined in several ways.

You can think of it as Lego money because you can build more complex DeFi products on top of existing blocks.

Identity

In collaboration with blockchain-based identity systems, decentralized finance protocols are an avenue to assist locked-out users formerly gain entry into a genuine global economic system. DeFi solutions help minimize collateralization needed for individuals who do not have the additional funds and assist users' creditworthiness through qualities around reputation and financial activity rather than conventional data points like income and ownership.

The DeFi world encourages data privacy surrounding personal identifying information, as well as free access. Therefore, anyone with an internet connection is free to gain access to DeFi applications while retaining control over their data and investments.

Gaming

The composability of DeFi has opened opportunities for product developers to create DeFi policies directly into platforms over a combination of verticals. Ethereum-based games have become a famous use case for decentralized finance because of their inbuilt economies and creative incentive standards. For instance, PoolTogether is a no-loss audited savings lottery that enables users to buy digital tickets by depositing the DAI Stable-coin, which is then combined and lent to the Compound money market protocol interest.

One of the main design principles of DeFi policies is compatibility, which refers to the fact that different system components can easily connect and interoperate. From the vast variety of integrated DeFi applications, one can see that the composable code has developed a powerful network impact in the community, which continues to build upon the things that other people have created. Many compare the process of DeFi development to building Legos. Thus, it has a famous nickname which is known as 'Money Legos.'

Ethereum developers and product teams can now build and initiate DeFi policies with the full package tooling and security integrations needed, especially from Truffle's smart contract liberties, Infura's API suite, and Diligence's security tools.

Data and analytics

Due to their phenomenal translucency around transaction data and network activity, DeFi policies give distinct benefits for data discovery, analysis, and decision-making around financial opportunities and risk control. The erratic growth of new Decentralized Finance Applications has stimulated various instruments and dashboards like DeFi Pulse and CoDeFi data. This helps users trace the value locked on DeFi policies, check out the platform risk, and differentiate yield and liquidity concepts. CoDeFi data is in charge of distinguishing yield from liquidity and other factors across the DeFi policies.

DAOs

Decentralized autonomous organization (DAO) cooperates according to the transparent regulations encoded on the Ethereum blockchain, thereby eradicating the desire for a centralized and organizational element. Other popular protocols in the DeFi space like Maker and Compound have initiated DAOs to fundraise, manage financial operations, and decentralize administration to the population.

Compliance and know-your-transaction (KYT)

Obeying anti-money laundering (AML) and countering-the-financing-of-terrorism (CFT) depends on know-your-customer (KYC) guidelines in conventional finance. In the DeFi vacuum, Ethereum's decentralized infrastructure aids the next-generation obedience analysis around the behavior of contributing addresses instead of participant individuality. This know-your-transaction (KYT) tools enable us to assess risk in quality time and defend against fraud and other financial crimes.

Asset management

Crypto wallets like MetaMask, Argent, and Gnosis Safe enable you to effortlessly and safely communicate with decentralized applications to perform every task from buying, selling, and transferring crypto to gain

interest in your digital investment. You are the keeper of your crypto funds with DeFi.

This means that you own your data in the DeFi space and control it all by yourself. For instance, MetaMask classifies your seed phrase, passwords, and personal keys in an encrypted layout locally on your device so that only you can have entry to your accounts and data.

Market places

DeFi policies have seen a significant increase in online marketplaces' collection, allowing users to exchange products and services internationally from user-to-user. These include everything from freelance coding gigs, digital collectibles, or Non-fungible tokens to actual jewelry and apparel.

Payments

User-to-user payment is arguably the foundational use case of the DeFi domain and the blockchain ecosystem at large. Blockchain technology is wired so that users can safely and directly trade cryptocurrency without the presence of intermediaries. DeFi payment solutions build a more free economic system for the underbanked and unbanked populace and help big financial institutions streamlining market infrastructure and serve better wholesale and retail customers.

Prediction markets

Blockchain-based prediction markets impede the crowd's reasoning and help users vote and exchange value on the result of events. Market prices then become crowdsourced pointers of the odds of an event. An example of a popular DeFi betting platform is Augur; it accentuates prediction markets based on election results, economic events, sports games, to mention but a few.

Saving

Many DeFi apps offer interest-bearing accounts, which can be exponentially more than the conventional savings accounts type based on a dynamic interest rate linked to supply and demand when sealed into lending pool policies like Compound. Some popular saving apps are Argent, Dharma, and PoolTogether, a no-loss savings game whereby players get back all their money even if they win or not.

An activity that has erupted around these creative savings tools is ‘yield farming.’ Yield farming refers to users moving their inactive crypto investments around in various liquidity protocols to increase returns. The craze of excitement surrounding DeFi yield farming has motivated no shortage of memes.

Staking

As the Ethereum network changes to a Proof of Stake accord algorithm with Phase 0 of Ethereum 2.0, users now have the opportunity to stake their ETH and get rewards whether as validators or through the staking providers. Staking on Eth2 is similar to an interest-bearing savings account where stakes receive interest – rewards for assessing blocks on the Ethereum policies before it gets appended to the blockchain.

Tokenization

This is one of the fundamentals of decentralized finance and an aboriginal function of the Ethereum blockchain. Tokens do not only power the network but also opens a diversity of economic possibilities. Simply, a token is a digital asset that is developed, granted, and directed on a blockchain. Tokens are built to be safe and immediately movable, and programmed with a span of inbuilt functionalities.

Ranging from real estate security tokens that illustrate fractionalized properties to platform-specific tokens that motivate using a particular application, Ethereum-based tokens have risen as a safe and digital choice for users worldwide the world to access, exchange, and store value.

Trading

In the DeFi space, trading comprises a range of derivatives trading, margin trading, and token swaps. This occurs all over an ever-growing and merged network of trade, liquidity pools, and marketplace. Crypto traders on decentralized exchanges profit from lower exchange fees, rapid transaction settlement, and full ownership of their assets.

DeFi vs. CeFi

Let's compare the key differences between DeFi and CeFi, meaning central or

traditional economy, but if you've already done that before, hit the share button to let this channel grow.

DeFi	CeFi
Permissionless	Permission-based system
Does not require knowing your customer protocol (KYC)	Requires to Know Your Customer
Open source - encouraging free collaboration	Closed source -decisions made behind closed doors
DeFi is generated on the blockchain	CeFi is generated on old foundations
DeFi is cheaper, mostly network fees	CeFi is more expensive-intermediaries charging hefty fees
DeFi is censorship resistant	CeFi can be censored

Differences between DeFi and Open Banking

When we talk about open banking, it is referred to as a banking system by which third-party financial enablers are provided with safe access to financial data through APIs. This helps with the connection of data and accounts between financial institutions and banks. It permits new kinds of goods and services within the conventional financial system. On the other hand, DeFi recommends a completely new financial system free of the present infrastructure. Sometimes, DeFi is referred to as Open Finance.

For instance, while open banking could permit the surveillance of all conventional financial instruments in one application by getting data from various banks and institutions securely, DeFi, on the other hand, could allow the surveillance of the completely new financial instruments and the new ways of communicating with them.

You can also refer to DeFi as “Lego money” because you can pile up dApps to increase your returns. For instance, you could purchase a stable-coin like

the DAI, then go ahead to lend it out on Compound for the sole purpose of earning interest. The fun fact, you don't need to look for any other gadgets as long as you have got your smartphone, then you are good to go.

Although most DApps found today are niche, still future applications may greatly influence daily life and activities. For instance, you will be able to buy a car or a house on a DeFi program under a mortgage agreement where you have to pay back for a stipulated time (months or years). The deeds or paperwork would be put up in a tokenized form on a blockchain record as collateral, and if by any means you stopped giving up your repayments, then the deeds or paperwork would naturally belong to the new owner, which is the lender. Due to a sense of lawyers or banks, the entire procedure of buying and selling the house or car becomes cheaper.

Why the Hype?

First, DeFi has been able to excel in this space with regulators behind the curve. For example, in conventional unsecured lending, there is the need for legitimacy in that the lenders and borrowers become acquainted (know one another's identities) and that the lender has the right to assess the borrower's financial sheet to be sure of their tendency to repay the debt owed. However, in DeFi, such requirements are not necessary. Rather, they are all about reciprocating trust and maintaining privacy.

Now, regulators have to weigh the fragile balance between suppressing innovation and flunking to protect the society from risks like people putting their money into a space that isn't regulated or banks and other financial organizations that are not capable of making a living as intermediaries. However, it seems that embracing change is the more sensible way to go, as is currently happening today. The US Securities and Exchange Commission (SEC) made an important change towards adopting DeFi by authorizing an Ethereum-based fund, Arca, for the first time in July 2020.

Since one of the major challenges concerning financial invention is the aggressive setting created by old regulations written for a foregone era, this change is very important and welcomed. Some of these regulations had caused some DeFi projects not to succeed, including the major ones like New-Jersey-based Basis, which refunded 133 million USD to investors in

2018 when it was finalized that it couldn't work within the SEC rules. Second, the mainstream players are getting involved, hence the rise of DeFi. Most high-street financial organizations are starting to approve of DeFi, and are looking for ways to take part in it. For instance, 75 of the world's largest banks are trialing blockchain technology to accelerate payments as a fraction of the Interbank Information Network. This is initiated by JP Morgan, ANZ, and Royal Bank of Canada.

Also, dominant asset management funds are beginning to take DeFi seriously. The most well-known that falls under this category is Grayscale, the world's biggest crypto investment account. It is managing over 5.2 billion USD of crypto investments, including 4.4 billion USD of Bitcoin.

The third is the impact of COVID-19. The pandemic has steered global interest rates even lower than it was before. Some jurisdictions like the Eurozone and the likes are now in the negative region. Others, including the US and UK, could probably come next if care is not taken in the expansionary monetary and fiscal policies being implemented to combat the surge in unemployment rates induced by layoffs due to COVID-19.

In this mood, DeFi gives much higher returns are potentially offered to savers than the high-street financial organizations. For instance, Compound has been offering a yearly interest rate of 6.75% to those who save with Stable-coin Tether. In this case, not only do you receive interest on your savings, but you also get to be a recipient of COMP tokens, which is an additional attractive incentive. With DeFi, you don't have to worry about having a bank account; have a smartphone in your possession, and finance will be opened to you on a platter of gold.

Lastly, there has been an increase in people putting their money into DeFi tokens because people refuse to be left behind and denied their exponential growth potential. We see lots of unreasonable exuberance these days because many tokens are worth nothing or nearly nothing when viewed practically. Whether you agree or not, we are headed towards a new financial breakthrough that is more free and decentralized than ever before. The big question is; how do we best steer its development with checks and balances to reduce the risks and circulate the probable advantages as broadly as possible? This is the challenge that threatens to fruit in the next few years.

Benefits of DeFi

Decentralized finance uses the Ethereum blockchain's major standards to maximize financial security and translucency, open liquidity and growth opportunities, and consent to an integrated and organized economic system.

Programmability

Smart contracts that are extremely programmable automate performance and encourage new financial tools and digital investments.

Immutability

Change-proof data coordination across a blockchain's decentralized architecture heightens safety and audibility.

Interoperability

Ethereum's comparable software stack makes sure that DeFi policies and applications are designed to incorporate and complement one another. Developers have the flexibility to create on top of existing policies, customized interfaces and integrate third-party applications with DeFi. Hence, people often refer to it as the money Legos.

Transparency

All transactions are broadcasted to and validated by the users on the network on the public Ethereum blockchain. It is important to note that Ethereum addresses are encrypted keys that are pseudo-anonymous. The degree of translucency around data transactions is highly desirable due to its rich data insights and high availability provided by a network that is accessible year-round with no downtime. Ethereum and DeFi policies running on it are also created with open source code available for everyone to see, audit, and create.

Permissionless

Contrary to conventional finance, DeFi is characterized by its open and does not require permission to access. Anybody with a crypto wallet and an internet connection can gain access to DeFi applications on Ethereum regardless of their location and often without any reduced amount of funds expected.

Self-custody

Using a Web3 wallet like MetaMask to communicate with permissionless

financial applications and policies makes DeFi market parties always control their data assets and regulation.

Advantages of DeFi

Usually, finance depends on banks acting as a middle man and courts to judge if the need arises. However, DeFi applications do not need arbitrators or intermediaries. This is because the code dictates the solution of every possible dispute that may ensue, and the users make sure to control their funds all the time properly. This method reduces the cost affiliated with giving and making use of these products and gives way for a more frictionless financial operation.

The moment these new financial services are installed onto the blockchain, there is the expelling of single failure points. Afterward, the data is documented on the blockchain and circulated across multiple nodes, eliminating the probable shut down of service, something not so easy to accomplish. The fact that the frameworks for DeFi applications can be created beforehand makes using one less complex and secure.

Another important merit of such an accessible ecosystem is the simplicity of access for users who, on a norm, would have no access to any financial services. Since the usual financial system depends on the intermediaries to make profits, their services are usually nonexistent in locations with low-income constituencies. However, the costs are majorly lessened with DeFi, and individuals with low-income can also be beneficiaries from this faster range of financial services.

DeFi and Potential Risks

DeFi, as good as it may sound, also faces some challenges that should be discussed with individuals that may be interested. This is to make you aware of what you are getting into properly.

Before moving on to this section, it's worth also mentioning the potential dangers of DeFi. One of the biggest risks is errors, bugs, and vulnerabilities in smart contracts and protocol changes that can affect existing contracts. For the same reason, consumers need additional insurance to reduce the risk of potential problems. Also, you should always check how decentralized your

DeFi project is and what the shutdown procedure is when something goes wrong.

An individual may have an admin key that can disable the protocol, or there may be a contactless management system that makes such decisions. Also, it would help if you always considered the more systematic risks that may arise from, for example, sudden depreciation of the price of an asset. This can lead to cascading liquidations through multiple DeFi protocols. Network and congestion charges can also be an issue. This is especially true if we avoid liquidation and try to provide more security on time.

The upcoming Ethereum 2.0 and Tier 2 scaling solutions can help solve this problem. It also has subtle features or changes that apply to one of the protocols, leading users to take less obvious actions that can cascade across multiple protocols. A good example of this is the recent increase in Compound protocols' composition, which forced consumers to engage in seemingly unprofitable loans at high-interest rates, profitable due to the additional COMP's compensation. These situations can be very dangerous, but as you have already noticed, they make the entire ecosystem more powerful and less sensitive to similar situations in the future.

DeFi is a fascinating and lively space full of opportunities, but it's important to remember that this is still a fairly new and emerging industry. Therefore, it is a game that has high risk and high reward. DeFi, unlike most tech companies, is almost a real mess for the traditional financial industry. DeFi does not rely on old techniques and procedures. It is based on new rails.

Currently, most financial products can only be made by banks. DeFi is open source, does not require authentication, and enables Internet-like collaboration. DeFi is primarily based on Ethereum, which uses more interoperability protocols, but we can see that more projects will be built on different chains in the future.

Here are some of them boldly highlighted:

- Poor performance

Blockchains are naturally slower than their centralized partners, extending to the applications founded on top of them. Therefore, there is a need for the DeFi application developers to take note of these restrictions and improve

their products accordingly.

- User errors

The liability is transferred from the intermediaries to the users by DeFi applications. This means that you are in control all by yourself due to the lack of central authority, which can quickly become negative for many users. To design a product with little or minimal risk of user error is a specifically hard challenge to overcome, especially when the products are placed on top of rigid blockchains.

- Bad user experience

At the moment, making use of DeFi applications needs extra effort on the part of the user. DeFi applications must deliver a substantial advantage that motivates and encourages users to change over from the conventional system ways. This will help them become a central component of the international financial system.

- Chaotic ecosystem

Finding the perfect and most suitable application for a particular use case can be quite challenging. However, users should find the time and possess the ability to discover the best scenarios at all times. The difficulty does not arise only when building the applications but also when thinking about how they can fit into the wider DeFi ecosystem.

Chapter 5: What Does Yield Farming In Decentralized Finance (DeFi) Mean?

As the exciting new financial sector's progress continues, consumers' trend to participate in protocol growth has increased. Whether it's as simple as introducing a cryptocurrency to Compound for something more complex, like participating in Maker's liquidation auction, DeFi is opening up exciting new passive income opportunities.

The yield farming technique is evolving and experimental, but the implications are amazing. On the general internet, you can't buy a product unless you give the website owner enough data required to activate the transaction, but with DeFi, you can borrow money without even disclosing your name or any personal information. The DeFi app doesn't care because it has the collateral it provides to secure the debt (e.g., a \$10 loan will require collateral worth about \$20 on the Compound platform).

If you follow this advice and decide to experiment with it, you can change everything back as soon as you do it, say after 10 minutes. However, it is still a good experience for someone who's all curious about the unique benefits Yield farming offers.

So, why lend money to people who already have it? Most people do this for some sort of trading. The most obvious example is shorting the market (to make a profit when the price drops). It's also great for those who want to stake tokens and at the same time engage in trading in the marketplace.

Don't You Need A Lot of Money To Run A Bank?

This is true, and on DeFi, this money comes primarily from strangers on the internet. That's why it provides a smart way for these decentralized banking apps to attract empty HODLers.

Liquidity is a major issue for all of these products. In other words, how much fund was staked in the smart contract? For some product types, the product experience is best with liquidity. Instead of borrowing from venture capitalists or debt investors, they borrow from consumers, says Avichal Garg,

Senior Partner at Electric Capital.

Use Uniswap, for example. Uniswap stands for Automated Market Maker or AMM (another term for DeFi art). In short, Uniswap is a web-based robotic system that is constantly ready to buy and sell any crypto coin that has a marketplace.

Uniswap has one or more marketing pairs for almost every Ethereum token. Behind the scenes, this means that Uniswap can pretend to be shopping directly with two tokens. This can be easier for consumers to do, but everything is based on a pool with two tokens. And each of these market pairs performs better in a larger pool.

What Do Pools Mean?

Let's take a look at how Uniswap works to show why more money helps. Let's say there is a market for USDC and DAI. The two tokens are stable coins, but they have different mechanisms for storing their value, and each one of them costs 1 USD. This commonly occurs in either of the tokens.

The price Uniswap displays for each token in a single market pair is based on the balance for each token in the pool. For example, if someone needs to create a USDC/DAI pool, both will have to deposit the same amount to simplify it. For a pool with only 2 USD and 2 DAI, the price is \$1 for 1 DAI. But imagine someone depositing 1 DAI and pulling out 1 USD. Then there will be 1 USD and 3 DAIs in the pool. The pool will be fine in order. Experienced investors can easily earn \$0.50 by investing \$1 and earning 1.5 DAI. This is 50% of arbitration and is a limited liquidity issue.

By the way, that's why Uniswap prices are usually correct, as traders find some deviations in the larger markets and trade them very quickly for arbitration proceeds. However, if 500,000 USDC and 500,000 DAI are in the pool, 1 DAI for 1 USDC transaction has little effect on the relative price. This is why liquidity is so useful. Assets can be locked into a Compound platform for a small profit. Yield farming seems to attract a wider group of retail investors, and professional investors who are looking for ways to maximize profits are those who engage in yield-farming.

DeFi creates related effects, so the market requires additional liquidity.

Uniswap solves this problem by charging a small fee for each transaction. This is done by slightly reducing each transaction and leaving it in the pool (since DAI trades at \$0.997 after commissioning, increasing the pool total by \$0.003). This helps liquidity providers get a share from the pool when someone puts liquidity into the pool. If you have many trades in this pool, you earn more commission, and each liquidity pool's worth goes up.

And this brings us back to the token. Liquidity added to Uniswap is displayed as a token, not an account. Crypto Yield farming is a way to generate more crypto coins with another cryptocurrency. This all relies on using DeFi applications to lend your money to other people who use a set of predefined steps in a smart contract. In exchange for your services, you receive a commission in the form of cryptocurrency. It looks very simple, isn't it? Well, it's not as you may think.

Successful yield farmers utilize very complicated systems or strategies. They regularly move crypto coins between different lending markets to maximize profits. They will also be very secretive about the best farming strategies they use. Why? The more they reveal their strategy, the less effective it gets.

Yield farming is the forest plots of land Decentralized Finance (DeFi), where farmers engage in competition to grow the best crops. The DeFi (Decentralized Finance) movement has been at the forefront of blockchain innovation. What makes the dApps so special? They are not authorized, so anyone with an internet connection and a secondary wallet can interact with them. Also, dApps eliminate the need for custodians or brokers.

I can force it to work; why can I use the asset? So, how do high productivity farmers get their yields? I'll explain them all below.

Yield Farming: Overview

Profitable yield farming equally referred to as liquidity mining, utilizes cryptocurrency to earn interest. Simply put, this means staking crypto coins and receiving interest on the staked amount.

In a sense, this process is very similar in nature to the staking of coins, but it works differently with many background complications. Often, the users are known as liquidity providers (LPs) who add cash to the liquidity pool play a huge role.

The liquidity pool is just a smart contract with deposited money. LPs are compensated for providing liquidity to the pool. Awards can be earned through commissions generated from the underlying DeFi platform or other sources.

Some liquidity pools are rewarded with multiple tokens. These reward tokens will be deposited in other liquidity pools where you can earn rewards. You can already see how quickly an incredibly complex strategy can emerge. However, the basic idea is that liquidity providers invest in liquidity funds and are rewarded in return.

Yield-farming is commonly carried out with Ethereum's ERC-20 tokens, and rewards are equally generally of the ERC-20 token type. However, this may change in the future. Why? Currently, most of this activity takes place in the Ethereum ecosystem.

However, Cross-chain linkages and other similar improvements could make DeFi applications decouple from underlying blockchain platforms in the future. This means that any smart contract would be compatible with any blockchains that support the contract's functionality.

Farmers generally shift their funds considerably between different protocols in search of high yields. As a result, the DeFi platform can also provide other financial incentives to attract more capital to the platform. Like the central stock exchange, liquidity attracts more liquidity.

What Started The Product Boom? The sudden interest in yield-farming could be linked to the launch of Compound token (COMP), a complex financial ecosystem management token. The control token gives the holder governance right. But how do you distribute these tokens to make the network as decentralized as possible? A common way to launch a decentralized blockchain is to distribute these control tokens algorithmically as liquidity incentives. This means that the liquidity provider will farm the new token and that provides liquidity to the protocol.

Although the company did not invent yield farming, the release of COMP made this type of crypto distribution model more popular. Since then, other DeFi projects have provided innovative plans to bring liquidity to the

ecosystem.

What is TVL (Total Value Locked)?

The best way to measure the overall health of the DeFi farm is to monitor the TVL (Total Value Locked). It measures how many crypto coins are locked in the DeFi lending platform and other types of currency markets.

In a sense, TVL is the total liquidity of the liquidity pool. It is a useful metric to measure DeFi's health and the farm market as a whole. It is also an effective measure of comparing "market share" for different DeFi protocols. A great place to track TVL is DeFi Pulse. You can see which platforms have the most ETH or other staked crypto assets on DeFi. This can provide an overview of the current yield farming situation. And naturally, higher staked value results in higher yield farming operations. You can estimate the value of TVL in ETH, USD, or even BTC. Each offers a different perspective on DeFi's money market situation.

How Yield Farming Occurs

Yield Farming has a close association with an Automated Market Maker (AMM) model. It typically includes liquidity providers (LPs) and liquidity pools.

Liquidity providers invest their money in liquidity pools. This pool generates a platform of exchange where users can engage in borrowing, lending, or swapping tokens. Use of these platforms is charged as a commission and paid to the liquidity provider based on the equity in the liquidity fund.

Nonetheless, the operation can be very different. This is a new technology. You will undoubtedly see a new approach to improving your existing operations. Another incentive to add cash to liquidity funds besides fees could be the new token distribution. For example, you cannot buy crypto in small quantities on the open market.

Conversely, it can be generated by providing liquidity to certain pools. All distribution rules depend on the unique implementation of the protocol. Liquidity providers earn income based on how much liquidity they provide to the pool.

The deposited funds are usually stable coins backed by the USD; however,

this can vary. Some of the stable-coins frequently used in decentralized finance include DAI, USDT, USDC, BUSD, etc. Some protocols are coins that represent coins deposited into a smart contract or the system. For example, if you add DAI to Compound, you will get cDAI or Compound DAI. Insert ETH into Compound, and you will get cEthereum.

There can be several levels of implementation involved. You can send cDAI to another protocol that creates a third token representing cDAI representing DAI etc. These chains can be very convoluted and difficult to follow, but you can follow a simple 1:1 approach when starting.

How Is The Profitability Estimated In Yield Farming?

The profitability of yield farming is usually estimated yearly. This is an estimate of what you can expect for the year. The commonly used measures are the annual percentage rate (APR) and annual percentage yield (APY). The difference between the two is that APR does not consider the compound interest, whereas APY does. Putting these cases together means reinvesting your profits directly to generate more profits. Nonetheless, APR and APY can be utilized interchangeably.

It is worth remembering that these are only estimates and predictions. It is difficult to accurately measure short-term rewards because a highly competitive and fast-growing market, and rewards can change quickly. If the strategy works for some time, many farmers will seize the opportunity and probably stop producing high yields.

Since APR and APY come from the old market, DeFi may need to write its measurements to calculate revenue. Due to DeFi's fast pace, estimating your weekly or daily earnings can make a lot more sense.

DeFi and Collateral Deposits

If you are in an asset business, you usually have to provide collateral to pay off your loan. This acts as an insurance policy for the loan. How relevant is it? It depends on the protocol you are sending money to, but you may need to keep an eye on the level of security.

Protection for the open market may be revoked if the security value falls below the threshold required by the protocol. What can be done to avoid liquidation? An additional token can be added.

Again, each platform has its own set of rules for this, i.e., its mandatory collateral relationship. Also, you usually work with the concept of nesting or over-collateralization. This means that the lender will have to deposit more than they want to borrow. This minimizes the risk of sudden asset price fall in the marketplace, which would activate removing a large amount of collateral from the system.

So, let's say you need a 200% security rate for the lending protocol you use. That means you can borrow \$50 for every \$100 of the value you put in it. However, it is generally safer to add more collateral than necessary to reduce the risk of liquidation further. That said, many systems use very high parallel ratios (e.g., 750%) to make the entire platform relatively safe from liquidation risks.

The Dangers Inherent In Yield Farming

Succeeding as a yield farmer is not an easy task. The most profitable growth strategies are very complex and are only recommended for advanced users. Also, Yield-Farming tends to be more suitable for people who can stake large amounts of crypto known as “whales.”

You must know what you're doing so as not to lose money. Besides the liquidation of your staked funds, let's see another risk associated with yield-farming. One of the obvious dangers of yield-farming is a smart contract. Due to the nature of DeFi, small teams create and develop many protocols on a limited budget. This can increase the risk of perceptual contract errors.

Even with large protocols audited by reputable audit companies, weaknesses and errors continue to be discovered. The tamperproof and immutable nature of the blockchain can lead to the money getting locked indefinitely in a defective smart contract. But with more platforms being created for smart contracts every day, we can easily see new startups create a layer of abstraction that gives you a test period for the contract before it's posted to the blockchain. This should be taken into account when staking funds in smart contracts. One of DeFi's greatest benefits is also one of its greatest issues. That is the issue of composability. Let's see how this happens.

As discussed earlier, the DeFi protocols are free and can be easily integrated. This implies that the entire DeFi ecosystem is highly dependent on each

building block. It also implies that the applications are composable and easily work together. Why is it dangerous? Well, if one of the building blocks doesn't work properly, the entire ecosystem can be affected. This is one of the greatest risks to farmers and liquidity pools. You have to trust the protocol that deposits your money and all the other interacting inner components in the system.

Crypto Yield Farming Platform and Protocols

How do we earn yield-farming rewards? There is no special laid down the process to do high-yielding farming. The strategy can change over time. The strategy and rules vary across platforms, and each of these comes with peculiar risks. When starting as a novice yield farmer, the first thing to do is familiarize yourself with the decentralized liquidity protocols' operations.

The basic premise is when you invest money in smart contracts, you get rewarded in return. But the actual practice can vary considerably. Therefore, generally, it's not advised to invest more money than you can afford to lose as a novice without first knowing the rules and risk management strategies. Having said this, we will now discuss the most popular platform for Yield farming. This is not an exhaustive list; it is just a set of protocols that are important to developing your yield-farming strategy.

Compound finance (COMP)

COMP is an algorithmic currency exchange where consumers can borrow and stake assets. Anyone with an Ethereum wallet can stake assets to a Compound liquidity pool and receive immediate rewards for the staked amount. Prices are adjusted algorithmically according to supply and demand. COMP is one of the most important protocols in yield-farming technology.

Yield farming of compound

Platforms used: Maker, Composite, Curve, and InstaDapp.

- Increase your COMP assets by optimizing your plans with Stable-coin.
- Open Vault and receive DAI by inserting ETH through Oasis Borrow (Maker).
- Open your DeFi Smart account in InstaDapp and insert DAI.
- Move the newly added DAI to the InstaDapp Composite section.
- Use InstaDapp's "Maximize Profit COMP" feature to take advantage of

- the DAI rankings offered for DAI assets.
- Option: DAI directly to the connection
- Note: When using InstaDapp's strategy, it can be thrown if the security is below the threshold.

The recommended ratio when using this strategy is 60%.

MakerDAO

Maker is a decentralized lending platform that supports the creation of DAI, a Stable-coin that is algorithmically linked to the value of the US dollar. Users can open Vault Maker to lock secure assets like ETH, BAT, USDC, or WBTC. They can generate DAI as a loan against the staked security. This borrowed amount overtime accrues interest known as a stability charge which the holders of MKR token determine. Yield Farmers can utilize the DAI Mint Maker for their yield-farming strategies.

Synthetix

Synthetix is a synthetic asset protocol. Anyone can securely deposit or stake Synthetix Network Token (SNX) or ETH and issue Synthetix assets for it. What is a synthetic asset? Almost everything has a stable price flow. This allows you to add virtually any financial asset to the Synthetix platform. Synthetix can use all types of assets for upcoming yield farming. If you plan to utilize a long-term gold bag for your Yield-farming strategy, synthetic assets can be suitable options.

Aave

Aave is a decentralized lending and staking protocol. Interest rates are adjusted algorithmically according to the current market conditions. The lender receives a token in exchange for funds. These deposited cryptos start earning interest and accruing compound interest upon deposit. Aave can also use other advanced features like instant loans. Aave, a decentralized lending and lending protocol, is widely used by crop growers.

Uniswap

Uniswap is a DEX (decentralized exchange) protocol that allows you to exchange untrusted tokens. Liquidity providers stake equal value of two different tokens to create the exchange platform. The trader can then trade

against this liquidity pool. In exchange for providing liquidity, the liquidity provider receives a fee for transactions occurring in the fund.

Uniswap is a widely used protocol to exchange tokens without trust due to its hassle-free nature. The use of Uniswap or similar methods is a strategy that can be useful for yield-farming.

Curve Finance

Curve Finance is a decentralized exchange protocol specifically designed for the efficient exchange of fixed currencies. Unlike other Uniswap-like protocols, Curve allows users to exchange expensive fixed coins with a comparatively lower slippage. As you might have guessed, the Curve pool is an important part of the framework as it is rich in Stable-coins for Yield farming.

The curve is a popular automated market maker platform that provides a very efficient way to redeem tokens while maintaining low fees. It maintains lower slippage by just supporting asset-only liquidity pools. While this approach lowers fees for liquidity providers that provide token pools, Curve encourages participation by integrating with external DeFi protocols and providing rewards in the form of CRV and interest rate tokens.

Yield Farming of Curve Bitcoin

The platform utilizes Ren Protocol, Curve, Synthetix, and the Balancer earns SNX, REN, BAL, and CRV to secure Curvepool sBTC liquidity.

- Transfer Bitcoin to Ethereum using Ren Bridge
- Enter the newly acquired renBitcoin into Curvepool SBitcoin
- Submit SBTC tickets through Mintr in the LP Rewards sector.
- Get prices in the form of SNX / REN balancing tokens.
- Get SNX and/or REN rewards on your balance sheet.

CRV liquidity mining on the curve platform utilizes Curve, Synthetix, Protocol Ren, and yEarn. Increase your CRV revenue with the Curve and Curve DAO liquidity indicator series.

- Pay the collateral to one of seven curves liquidity pools.
- Those wishing to participate in a Bitcoin pool use the Ren protocol to transfer BTC to Ethereum.
- Invest in liquidity tokens through Curve evaluation.

- To increase liquidity, we secure CRV and lock it utilizing Curve DAO.
- Find additional incentives such as SNX and REN for sUSD and sBTC pools.

The curve is an automated market maker platform similar in many ways to Uniswap and Balancer, except that it only supports liquidity pools containing assets with similar behavior, such as fixed coins, or those u-packaging similar assets as wBTC and tBTC. This approach allows Curve to use more efficient algorithms and offer the lowest charges, slippages, and volatility losses on any decentralized Ethereum exchange.

Balancer

A balancer is a Uniswap and Curve liquidity protocol. However, the main difference is that liquidity funds can adjust the distribution of tokens. This allows liquidity providers to create their balanced pool instead of the 50/50 split required by Uniswap. Like Uniswap, LPs receive fees for transactions occurring in liquidity funds.

With the flexibility to build liquidity, Balancer is an important innovator in crop growing strategies.

Balancer liquidity mining

The platform connects your capital to Balancer's liquidity pool to earn BAL control tokens. Use a prediction table like Predictions exchange to determine which pool receives the most BALs based on the total percentage, where 1 is the highest possible ratio.

- Visit <https://pools.balancer.exchange/#/> o invest capital in the selected pools.
- Pro Tip: A pool that temporarily reduces losses is recommended. This includes 1:1 linked pools such as sETH/wETH, sBTC/wBTC, and DAI/USDC.

Yearn finance

Yearn.finance is a decentralized ecosystem of collectors for credit services like Aave, Compound, etc. It aims to find the most profitable loan services algorithmically and optimize crypto loaning. Once deposited, the cash is converted into tokens and is regularly balanced to maximize profits.

Yearn.finance is useful for farmers looking for a protocol that automatically selects the optimal strategy.

Chapter 6: Ways to Mine Your Bitcoin on Your Own

There are three ways to get Bitcoin; by purchasing on an exchange, collecting them for goods and services, and last one is by mining new ones. Bitcoin acts like cash, but it can be mined into gold. “Mining ‘is a language used for the discovery of new Bitcoins – just like discovering gold. It is the validation of Bitcoin transactions compiled into one block with a fixed size and added to the blockchain in real life.

For instance, Cynthia purchases a TV from an online retailer with a Bitcoin. To make sure her Bitcoin is real, miners perform a computational operation that is specific to each blockchain to validate transactions and add new blocks of transactions. The validation process is more complicated than that, but to keep it simple, we will think of it in the simplest words as validation of transactions. All the transactions are compiled in blocks with a virtual padlock called the “blockchain.” Miners then run the software to find the key suitable for opening this padlock to add new blocks.

When their computer finds this key, the box will open, and the transactions will become verified. The reward for finding the suitable key fit to unlock the padlock amounts to 12.5 newly generated Bitcoins, that value halves every certain number of blocks due to the predefined rules for bitcoin created by its pseudonymous inventor Satoshi Nakomoto. According to a top site for the latest genuine Bitcoin transactions, the present number of trials it takes to find the key is around 1,789,546,951.05.

Regardless of the huge number of trials, the reward of 25 Bitcoin is offered about every 10 minutes. However, mining solo nowadays is demoralizing because the process of looking for blocks is so popular, and the difficulty of finding a block is less to the point that you may have to set aside your machine for about three years before it can generate any coins.

Pooled mining, on the other hand, is far more productive. This allows you to split the work amongst a ground of people. All you need do is work for shares in a block, and when it is mined and appended to the blockchain, you get a percentage of the block based on the number of people or users you

worked alongside, with lesser fees inclusive.

Here are some steps to take so that you can start mining your Bitcoin with ease.

Get a wallet

You have the choice of either storing your wallet locally or online. You need to use or download a fairly huge blockchain file of about 320GB; downloading and updating a local wallet may be a no-no. The method which you decide to use to keep your Bitcoins depends totally on your personal preference. There is no perfect wallet type as they all have their upsides and downsides; however, privacy advocates would prefer a local wallet.

The moment you have created whichever wallet you like, you get an address like 1BEkUGADFbrEShQb9XJ. This is a direct way to send your Bitcoins to your wallet, so take note of it. You can find the wallet address under linked accounts in Coinbase.

Join a pool

You have to work with other miners on available blocks before you can mine a pool. Each pool is distinguished mostly by the fees they charge by block and the number of users. Pools with fewer users could also have a slower time to discover blocks that need to be mined, but pools with many users usually end in smaller payments.

There are simple guidelines for most services to avoid being overwhelmed. Also, ensure that you enter your wallet address into the pool info. This will make sure that you get your Bitcoins.

Get a miner

There are various mining options for different forums, and OSX users may find themselves in a bit of a pickle. Miners make use of spare GPU cycles to power the mining operation. Miners use these cycles to help take care of user-to-user processes related to Bitcoins. Therefore, you are handling the network as well by doing “work.” You can research more about this to get a clearer picture. And to give you a starting point, lookup ASICs (Application Specific Integrated Circuits).

Keep your mind on the prize – your money

Bitcoins are vastly simple to use and mine. You may think that you may be able to throw lots of machines together and gather Bitcoins like sand, but this is not so. The more Bitcoins are discovered, the more difficult they are to find. You will understand what you are up against by using one of the online profitability calculators for Bitcoin or Ethereum mining.

In summary, if it costs more to run your hardware than you profit in Bitcoins, then you are likely doing something wrong

Conclusion

DeFi circles around applications referred to as DApps, which means Decentralized Applications. These applications go-ahead to do financial functions on digital ledgers known as the blockchain, a technology that was first employed by Bitcoin but has since become broader than it used to.

Instead of transactions being made with and by a centralized intermediary such as cryptocurrency exchange, transactions are done directly between people, however, with the aid of smart contract programs. DApps are accessed through a WebCam3 browser extension or application like MetaMask, allowing users to interact with the Ethereum blockchain through a website.

Furthermore, most of these DApps can connect and work in unison to create detailed financial services. For instance, a Stable-coin holder can turn assets into a liquidity pool. Others will borrow from this pool by putting in additional collateral, usually more than the loan amount. Then, the policy necessarily changes interest rates based on the time-to-time claim for the asset.

Decentralization means the absence of a central exchange. Smart contract programs used for the DeFi policies themselves are operated with the aid of open-source software courtesy of a community of developers and programmers. An example of a DeFi policy is Uniswap. This is a decentralized exchange or dex that operates on the Ethereum blockchain and permits the trading of hundreds of various digital tokens that are produced on the Ethereum blockchain.

Instead of depending on the centralized market markers to fill orders, Uniswap's algorithm encourages users to create liquidity pools for the tokens by producing trading fees for the people providing liquidity. While the users entirely control the Uniswap platform, a development team is in charge of writing software for its deployment.

Direct purchases are not the only kind of transaction or contract controlled by big companies, other financial applications like loans, insurance, derivatives, betting, crowdfunding, to mention but a few, are also in their grasp. Therefore, taking away the middlemen from all these kinds of transactions is one of the main objectives of DeFi.

We have covered the latest cryptocurrencies, such as crypto farming and DeFi products. What else can this advanced economic revolution bring? We don't know what new applications will come in the future based on these current components. However, unreliable liquidity protocols and other DeFi products are at the forefront of economics, crypto-economics, and computer science.

DeFi's money market can undoubtedly help create a more open and accessible financial system that anyone with an internet connection can access, which will bridge the gap between our lives on earth and rely on the human factor to potentially reach living on Mars. At the same time, we generate passive income from yield farming on earth-based securities. In future parts of the "Stake Hodler Capitalism" book series we intend to cover many applications of blockchain in depth including, smart contracts, Internet of Things, Retail, Agriculture, and Manufacturing.