Blockchain, Cryptography and its future

Abstract

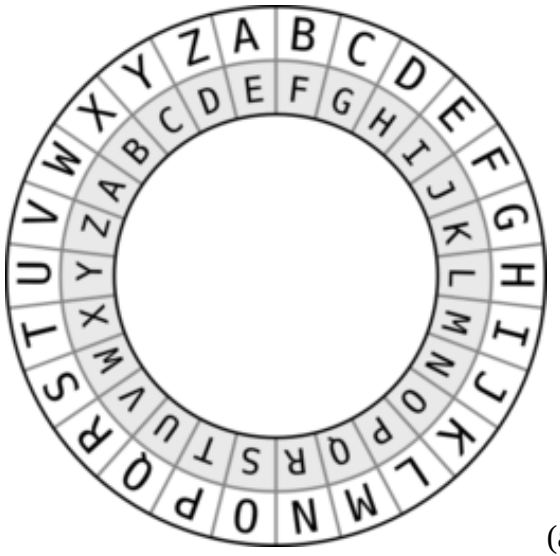
This paper is about blockchain, specifically topics relating to it such as money, math, and computer science. Specifically, I will be covering the math behind cryptography, machine learning applications in blockchain, Stable crypto currencies and lastly the future regarding blockchain.

Math in cryptography

Early in history, people were very interested in communicating with one another. Ways of communication started of from simple talking, until the 3000 BC the invention of writing and reading started to begin evolving humans and their ways of communication. With writing and reading, humans also developed their analytical abilities and eventually created mathematics. With these ways of communication, humans are also interested in sending messages intended for them to communicate secretly; this is the start of cryptography.

Before moving forward in cryptography, we have to note that cryptography is a branch of number theory so basic concepts of simple number theory such as natural numbers and GCD are expected to be seen here. Cryptography is essentially a way to protect communication, it makes unwanted individuals not understand what is being meant and only individuals that can encrypt it (transforms the crypted data into readable text)

Early on, cryptography algorithms were very simple and symmetric. They rely on a unique key that is used for both parties to encrypt the messages being sent. An example of this early, symmetric cryptography algorithm is a classic Caesar’s cipher.



(almightyguru)

This is a Caesar's cipher of n = 5, an example regarding this is, let's say there is 2 people named Abby and Bryan. Abby wants to send a message "hello" to Bryan. Using the Caesar's cipher to encrypt the message. First, Abby encrypts the message "hello" according to the cipher which gives "LIPPK" to Bryan. Knowing it's using the cipher, Bryan use the same cipher of n=5 to decrypt the "LIPPK". Following the cipher, Bryan gets back "HELLO" which was the original message intended by Abby.

Note that if Bryan or Abby used different n in Caesar's Cipher, they wont get the same message back. (n is the number of shifts of the alphabet of the outer ring, n = 0 means no shift thus Caesar's Cipher will be equivalent to the inner letters.)

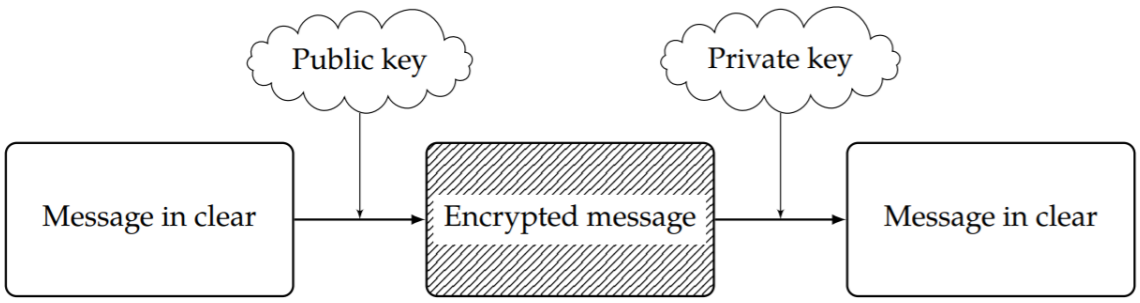
These algorithms are also used in historical events such as in the wars. One notable story is Alan Turing when he was trying to help the allies defeat the axis powers. He assisted in ciphering Axis power's messages that used the Enigma cipher machine, which was a symmetric algorithm. He eventually figured out the details of the Enigma cipher machine which is then used to intercept messages of the Axis power.

Moving forward from Caesar's cipher, we can see that these symmetric systems are not that secure which is not what we want in a cryptographic algorithm. Therefore, the invention of the asymmetric algorithm changed the course of cryptography and the future of it.

Asymmetric algorithm works very similar to a usual symmetric. However, Asymmetric algorithms allow to reduce this weakness of a symmetric algorithm by using two different keys:

1. A public key that is to be used for encrypting the message, this can be shared publicly without affecting the confidentiality of the message
2. A private key which is only for the selected recipient to decrypt the intended message

"The idea is that anyone can encrypt messages using the public key but only the recipient can decrypt them with his private key. Particularly, the knowledge of the public key should not be enough to decrypt messages. The main goal is that anyone can encrypt messages using the public key but only the recipient can decrypt them with his private key. Particularly, the knowledge of the public key should not be enough to decrypt messages unlike symmetric algorithms." (Campesato, 2020)



(Campesato, 2020)

A famous asymmetric algorithm is then created in 1977, by Ron Rivest, Adi Shamir and Leonard Adleman called the RSA Algorithm. (Initials of their surnames) RSA Algorithm works by consequences of number theory advancements over the years. Notably is that, (Euler's theorem) Let $n \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{Z}$ such that gcd(a, n) = 1. Then $a^{\wedge}\varphi(n) \equiv 1 \pmod{n}$. (Fermat Little Theorem is special case of Euler's: p is prime then $\varphi(p) = p - 1$).

First, we have to Generate the keys: pick two distinct prime numbers p and q. sets $n \coloneqq pq$ and then choose $e \in \mathbb{N}$ such that gcd(e, $\varphi(n)$) = 1. Then the public key is (n, e).
where $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ defined by $\varphi(n) \coloneqq \#\{k \in \mathbb{N} : 1 \leq k \leq n$ and gcd(k, n) = 1$\}$
Since gcd(e, $\varphi(n)$) = 1, e admits a multiplicative inverse modulo $\varphi(n)$, i.e. there exists $d \in \mathbb{N}$ such that $ed \equiv 1 \pmod{\varphi(n)}$. So, there exist u, $v \in \mathbb{Z}$ such that $eu + \varphi(n)v = 1$. Then we take $d = u + k\varphi(n)$ for a suitable $k \in \mathbb{Z}$ for d to be positive. Then the private key is (n, d). (Campesato, 2020)

Encrypt: Get the public key (n,e), note the message is going to be an element of $m \in \{0, 1, \dots, n - 1\}$ Then, there exists a unique $c \in \{0, 1, \dots, n - 1\}$ such that $c \equiv m^{\wedge}e \pmod{n}$. It is going to be the crypted message. David sends c to Chris, and Chris will use his private key in order to get m from c (Campesato, 2020)

Decrypt: From c, we now just have to solve $k \in \{0, 1, \dots, n - 1\}$ such that $k \equiv c^{\wedge}d \pmod{n}$.

(We claim that $m = k$. Indeed, since $ed = 1 + l\varphi(n)$ for some $l \in \mathbb{N}$, using Euler's theorem $k \equiv c^{\wedge}d \pmod{n} \equiv m^{\wedge}ed \pmod{n} = m^{\wedge}(1+l\varphi(n)) \pmod{n} \equiv m \times (m\ \varphi(n))^{\wedge}\ l \pmod{n} \equiv m \times 1^{\wedge}l \pmod{n} \equiv m \pmod{n}$) (Campesato, 2020)

In Practice: Chris wants to use the RSA Algorithm to try encryption with his friend. He picked the prime numbers $p = 13$ and $q = 17$ then $n = 221$ and $\varphi(n) = 12 \times 16 = 192$. Then he picks $e =$

11, which is a suitable choice since gcd(192, 11) = 1. Using Euclid's algorithm, Chris obtains the Bézout relation 192 × (−2) + 11 × (35) = 1. Therefore, she sets d = 35 so that $ed \equiv 1 \pmod{192}$. Then, he shares the public key (n, e) = (221, 11) to David and keeps the private key (n, d) = (221, 35) Later, David wants to send the private message m = 149 ∈ {0, 1, 2, … , 220} to Chris. Since public key (n, e) = (221, 11) he computes m^e = 149^11 ≡ 89 (mod 221). Therefore, the encrypted message is c = 89 ∈ {0, 1, 2, …, 220}. c = 89 is then sent back to Chris and he computes c^d = 89^35 ≡ 149 (mod 221) and he recovers the original message of m = 149. (Campesato, 2020)

After the RSA algorithm, there are a lot of other encryption related projects that came out too such as the SSL which is used in the internet and notably blockchain but how do we connect this 2 different fields together?

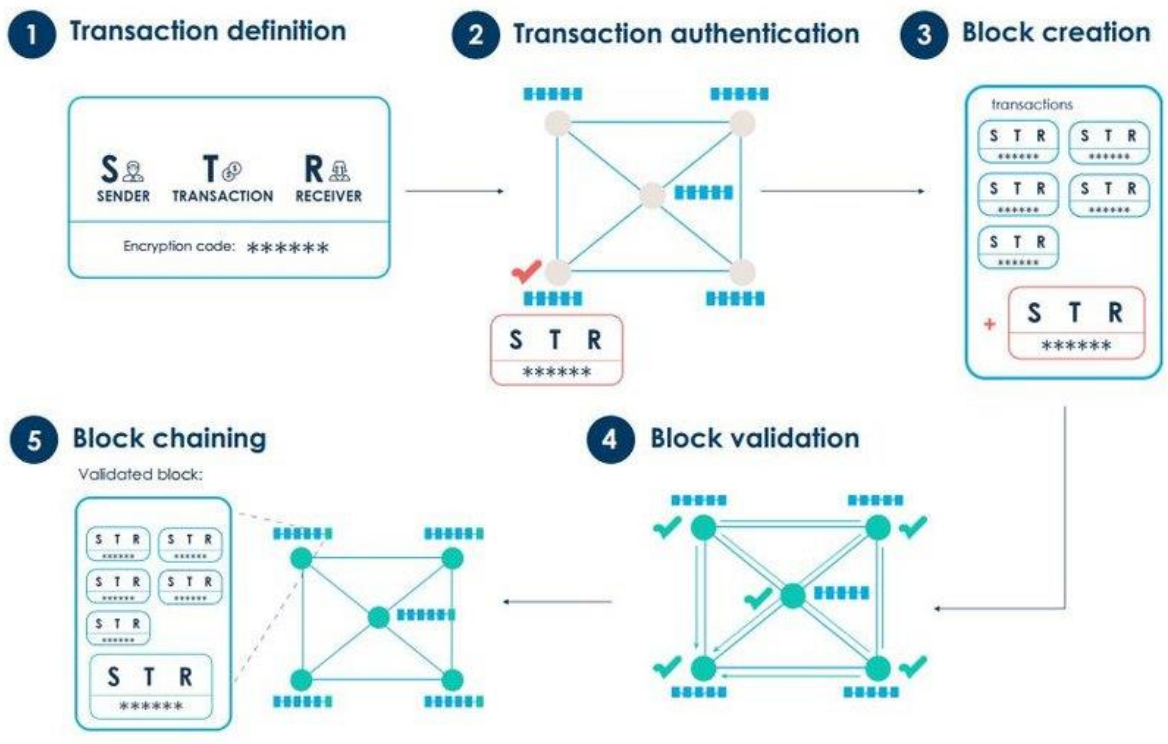
We must first introduce what is cryptocurrency/blockchain. A definition of blockchain from IBM states that "Blockchain is a shared and unalterable ledger that facilitates the process of recording transactions and tracking assets in a trading network. An asset can be tangible (a house, a car, money, land) or intangible (intellectual property, patents, copyright, trademark). Virtually anything of value can be tracked and traded in a blockchain network, reducing risk and costs for all parties involved" (IBM)

Blockchain place an essential role in cryptocurrencies as similar with the definition above it helps "maintain a secure and decentralized record of transactions. Blockchain innovation guarantees the fidelity and security of a record of data and generates trust without a third party needed." (Hayes, 2021)

Hence, cryptocurrencies rely on cryptic algorithms we saw above to be able to function properly. An example is a blockchain wallet, it uses asymmetric encryption to be able to function it as basically it's a collection of private keys to be able to sign transactions on the network.

With the development of blockchain, during 2009 a protocol called Bitcoin is built on a blockchain. When any transactions of bitcoin are made, everything is public as it is record in the blockchain. Blocks are like files which hold data of the network — and in a blockchain, they make a chain, each one dependent on the others.

But since blocks are like data files, larger blocks require more computation power to verify them. "Hashing" a block is the process of ensuring the validity of the network transactions and as a reward for hashing, miners receive bitcoins. (Becker, 2021)



(Froystad and Holm, 2016)

“A cryptographic hash function is a special type of function that takes an input string of a given length and converts it into an alphanumeric string of fixed length. In the case of Bitcoin, a “Message” is inputted, and a hash function, known as SHA-256 (Secure Hashing Algorithm 256), gives an output known as a “Hash”. This means that however long the string of data (limit of 2^{256}- 1 bits), the output will always be 256-bits in length. The process of hashing is not a method of encryption as it is only a one- way process and therefore cannot be reversed (decrypted); there is a billion-dollar prize to those that can find the inverse of SHA256.” (Chitty, 2020) To see how SHA works there is a table below showing the different outputs of the function. SHA-256 is also deterministic, meaning given the same input, the output will always remain the same.

Input in SHA-256	Output
“Math and Law”	33c674ef797860794ac235f3433b58b9eea0b295dcff7dcd2d72dbab70655bdc
“math and Law”	f87933fddbd135d5dc87b85eef46ba5e38fd0816778f4c1c8d45d0be480a0b4f
“law”	8f1f74adf65864c86d3d471ea8ca9e329d4282489edc156c99604264090774bf

Note that only 1 character was changed but the output changed dramatically and all outputs the same length despite the input.

Machine learning in blockchain

By looking at how bitcoin works, we can see there is a lot of data being stored and used to function as a protocol. Luckily, big data sets are very beneficial to be used for machine learning. This way protocols can learn and use this machine learning techniques to them more efficient and secure. As these algorithms helps to identify patterns and get insights of the data.

Following are some industries that uses blockchain and machine learning:

1. **Energy and Utilities**

   In the Energy and Utilities industry, blockchain is being used for the energy exchanges. LO3 Energy is one of these companies in this industry that uses blockchain technology to generate energy, conservation and trading for the community. They use microgrid smart meters with smart contracts to track and manage these energy flows. Using AI in these smart grids, it helps track the grids interactions with the different intensity of energy and optimally change the grid to increase the efficiency using machine learning.

   Another example is Verv. It is a blockchain focused energy application that uses machine learning to analyse electricity consumption of the users. Machine learning is then used to find anomalies in the system. If any is found, Verv will track how much you waste and try to find a solution for the user (identifying the spare part needed to be changed). The wasted energy is then labeled until a certain amount and the fault diagnostics will be sent to the relevant companies to help fix the issue.

2. **Food and Logistics**

This industry uses blockchain and ML to solve supply chain issues as by nature of this technology, both technology makes the process more accurate and transparent. Using blockchain, the food industry is able to track food supply chains and manage financial payments. A notable project in this space is when IBM and Twiga Foods collaborated to make a Blockchain-Based MicroFinancing for Food Kiosk Owners in Kenya. Twiga was interested in making a finance lending platform for these kiosk owners but had some troubles regarding these kiosk's credit scores. Therefore they collaborated with IBM to help build this. "We analyzed purchase records from a mobile device and then apply machine learning algorithms to predict credit worthiness, in turn giving lenders the confidence they need to provide microloans to small businesses. Once the credit score is determined, we used a blockchain, based on the Hyperledger Fabric, to manage the entire lending process from application to receiving offers to accepting the terms to repayment," (Kinai, 2018). Additionally, other multi national organizations such as Unilever and Nestlé are starting to think about using blockchain to deal with food disasters issues such as wastage and contamination.

3. **Manufacturing**

Advancements of the manufacturing industry made them use new technologies to make the process better. A new technology used is using blockchain processes and smart contracts for production, transparency, security and compliance checks of the company. Instead of static machine maintenance schedules, machine learning combined with the blockchain technology are used to predict these schedules in the most optimal time. QC

and testing of products are also mostly automated by machines (accompanied by AI and computer vision)

An example is Porsche, the German car company, leveraging Blockchain and ML to improve automobile capabilities and safety. The company uses blockchain technology to transfer data more securely and quickly. Whether they are parking, charging, third-party access needs like temporary access to a car, a parcel delivery agent all these things use blockchain in order to function as an ecosystem

Despite their uses in these industries, there are still advantages and disadvantages of using these new technologies. Notably, combining the 2 together we can see a lot of improvements in transactions fees and increasing security in the chain. With the larger number of data being stored and produced, with AI identifying fraud is very easy and transparent and finding the most optimal option is easy.

On the other hand, there are some disadvantages using them. We have to know even though a lot of data is being collected, is all of them useful for the AI to learn from? This huge amount of data might be a concern and an additional cost for the company to handle and store the data. For multinational companies, by nature of blockchain, privacy and security might be an issue for using blockchain. As there are still exploits being made in the blockchain system and privacy issue of the individuals using these services will be very transparent which rises questions regarding how much we can rely on these systems.

\

Stable coins and regulatory framework

From blockchain to bitcoin, we developed resources to make bigger and better protocols however due to the nature of the blockchain markets, cryptocurrencies are very volatile. These currencies are then not very suitable medium of transactions because of the rapid price changes. Stablecoins are then made to fight the volatility of these coins as they are made to offer price stability to the markets. It is also a way to maintain the decentralized nature of blockchain, participants doesn't have to use a centralized medium as a way to exchange their crypto to "fiat".

(Clark ,2021)

There are different types of stablecoins such as

- Fiat-Collateralized Stablecoins
- Crypto-Collateralized Stablecoins
- Non-Collateralized (Algorithmic) Stablecoins

Fiat-Collateralized Stablecoins are the closest thing in crypto to fiat currencies, they are usually pegged to the underlying asset (usually USD). These stable coins usually maintain a fiat currency reserve to act as a collateral for the stablecoin itself (Like a central bank). These reserves are typically not in blockchain but in a real bank account.

An example of a Fiat-Collateralized stable coin is Tether ($USDT), it was launch in 2014 and currently has 78 billion in total supply. They revolutionized the stablecoin industry and most of the stablecoins in the market today was formulated/influenced by Tether. In theory, to be able to peg an asset to USD, they must have a reserve 1:1 with the supply. However, we have to know that these reserves aren't fully regulated which we will cover more in the following paragraphs.

Crypto-Collateralized Stablecoins are another type of stablecoin that has a reserve used to maintain price. The invention of this is essential for the decentralized finance ecosystem. These coins collateralize digital assets instead of fiat currencies. Therefore, they algorithmically control the reserves in order to properly peg the price. In comparison with fiat-collateralized stablecoins with is prone to mispricing when huge, unbalanced volume is being transacted. These coins are like a loan (usually accompanied with yield rates), first we deposit the digital asset and it is then locked for a certain time in the chain. And to get back the collateral, we have to pay back the stablecoin into the smart contract. This is more decentralized then fiat backed as technically there is no connection between the coins and the centralized system.

MakerDAO ($DAI) is one of these crypto collateralized stablecoins. They use smart contracts to act like vaults for collateralizing the asset and giving out DAI tokens (the stablecoin). To get back your money, you just have to payback the DAI and by the smart contract you will have

your collateral back. Even though both DAI and USDT are stable coins, they still coexist in the defi ecosystem together serving different tasks.

Non-Collateralized (Algorithmic) Stablecoins probably the most different then the ones mentioned above as by definition it is not backed by any collateral (no fiat or crypto. Because they have no reserves to support the coin, it still has an automated system to help manage the stable price.

These coins work very similarly like a central bank of a country practising their fiscal/monetary policies. The coins supply often changes accordingly to the volume of the coin itself to help maintain the "stable" price of a stable coin using a smart contract. If individuals started to sell a lot of an algorithmic stablecoin, the smart contract will adjust itself and reduce the supply of the coin to help fight against the fluctuating supply and demand of the coin. (Works vice versa as well)

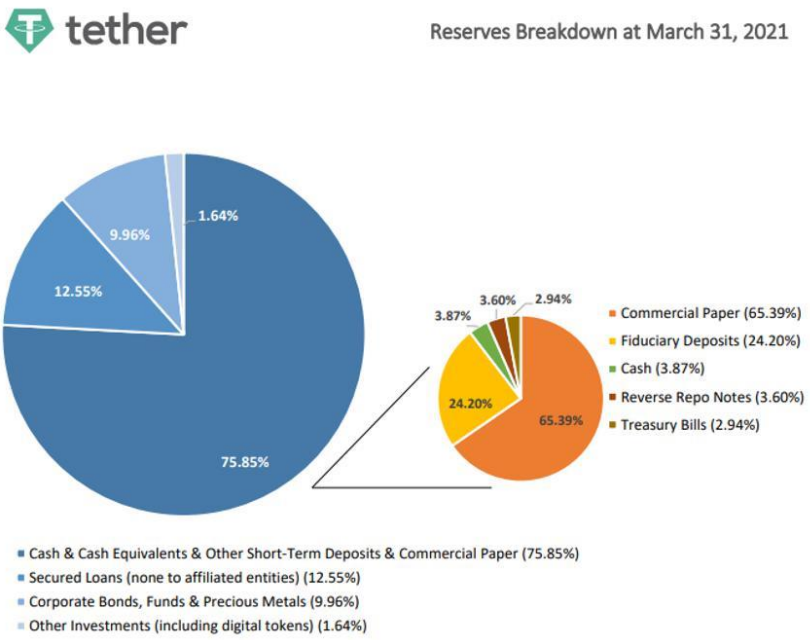
Stablecoin regulation problems

Back to tether being the first and famous stablecoin, they are attacked with a lot of controversy from their reserves and to allegedly manipulating crypto exchanges.

No one bats an eye about tether's reserves until recently when they were asked to be audited. For years, tether reported that all the tokens are backed by a dollar in the reserves but as shown in the diagram below, only 3.87% of the total supply was backed by fiat. This is certainly misleading for the public and so regulators steps in the system. Particularly the CFTC (Commodity Futures Trading Commission), gave out a statement after the findings that states, "This case highlights the expectation of honesty and transparency in the rapidly

growing and developing digital assets marketplace." (Robinson, 2021) With that being said tether is then fined $41 million to settle against the allegations of their misleading assets and Tether didn't admit or deny the CFTC's allegations

Another issue that tether made was with the collaboration with the famous exchange Bitfinex. Bitfinex was one of the early cryptocurrency exchange mostly trading bitcoin made in 2014. However due to several mistakes they made during 2017-2018 they suffer from huge losses to upwards of $70 million because of the bitcoin crash and a security breach that stole over 119,756 units of Bitcoin which was about $72 million at the time. Coincidentally, Tether and Bitfinex shares similar shareholders and management and therefore, they both worked together to cover bitfinex's losses. (Note at this time, everyone thought tether was backed 1:1 with the USD, but we know recently that isn't the case) Therefore sparked a lot of noise from the community regarding this issue. Both Tether and Bitfinex were $18.5 million fine without admitting or denying the allegations.



(Gans, 2021)

The story doesn't end there regarding Bitfinex and Tether. By design of blockchain and its transparency, colleagues from the University of Texas started digging about bitfinex's transactions. They found that during 2017 the bitcoin price gain was artificially made by bitfinex "creating price support for bitcoin" They found that "about 87 hours, or about 1 percent, of heavy tether trading could explain 50 percent of the rise of bitcoin, and around 64 percent of the rise of other major cryptocurrencies." (Rooney, 2021)

Future of blockchain

We saw the origins of blockchain, its applications and its regulations regarding stable coins. But what is next in blockchain?

Blockchain is being used as it was a way to send "money" over the internet. (Bitcoin) With the advancement of the technology, new blockchain protocols began to emerge; notably is Ethereum. Ethereum was the first blockchain protocol that uses smart contracts and creation of decentralized applications to use their network. Ethereum revolutionized cryptocurrencies and is why crypto is the way today.

Smart contracts are not like contracts that lawyer make which are long terms and conditions of legal document. Contract here is just an agreement between parties. Smart contracts are then just "digitize agreements by turning the terms of an agreement into computer code that automatically executes when the contract terms are met." (Ethereum). This smart contract helps "Ethereum to be used to codify, decentralize, secure and trade just about anything you can think of." (Hayes, 2021) These smart contracts are then further developed into tokens (ERC-721, ERC-20, and many more) and these tokens building blocks of Ethereum we see today.

The most common usage of a smart contract is with the ERC-20 token (Ethereum Request for Comments 20). ERC-20 is a standard for fungible tokens, which basically means one token is equal to another token. Let's take DAI as an example, if we both exchange DAI, at the end of the exchange we still have DAI (no changes in token). ERC-20 tokens as it is fungible are very similar to other crypto currencies like bitcoin. These tokens can be sent and received and if there is a liquidity pool regarding the assets, these tokens can be exchange to different tokens (like selling eth (erc-20) to usdt, if there is a eth/usdt liquidity pool) Liquidity pools are this pool of tokens (usually in pairs ETH/USDT, BTC/USDT, etc.) which are located in a smart contract which is then used to facilitate trades of the assets and the exchange. The only difference of a ERC-20 token and other tokens like bitcoin is that ERC-20 token exists in the Ethereum ecosystem and not their respective networks like a typical blockchain.

These tokens are very close to the defi movement. DeFi is short of decentralized finance which is a term that disrupts centralized finance. Since they not controlled by a single party like the government/central bank, but among a group of computers in the blockchain. (Liquidity pools are usually created by members of the community of the erc-20 token usually a yield is given back to the liquidty providers, note that not one person controls the liquidity pool as its all in the smart contract)

ERC-20 are also used with smart contracts to make Dapps in Ethereum (decentralized applications). These Dapps are the interesting applications made in the Ethereum network, from yield farming to peer-to-peer gambling websites there is no limitations on what you can build in DeFi.

A protocol named Olympus DAO is a good example of a defi application in the Ethereum Network. Olympus DAO ($OHM) is a decentralized reserve currency protocol that took

inspiration of the stablecoins structure we saw before. They modified the structure as a way to combat inflation and liquidity problems of the stable coins. Olympus DAO's ERC-20 token $OHM is made out of these baskets of digital assets, and so in theory $OHM will remain stable and appreciate more compared to stable coins; fighting against inflated as they wanted.

In order to do this, Olympus DAO uses 2 ways to sustain in the DeFi ecosystem, experts even states that Olympus DAO introduce DeFi 2.0 to the ecosystem. The 2 ways are to Stake and/or Bond. When staking, the individual lock their $OHM for a time frame. They will receive back sOHM as a yield reward. And if the individual wants to take profit the sOHM is burnt maintaining the supply (less risk of inflation of OHM). In Bond, Olympus DAO offers individuals $OHM for less price than market, but they have to lock their collateral for a period of time. (Olympus)

When the reserve of the DAO increase, Olympus can make more OHMs to make prices stable or higher. Olympus DAO is an example of a dapps as it is revolutionary and offers a 5000% annual percentage yield for people staking their OHMs.

A DAO stands for decentralized autonomous organization is an organization with no main leadership. Decisions are made from any one in the DAO, but these proposals must be approved by a group vote to be implemented. Essentially, DAOs are publicly owned by the community (like a public owned company with no hierarchy voting powers) Some even like to compare DAOs to venture capital firms that are "based on open-source code and without a typical management structure or board of directors. To be fully decentralized, a DAO is unaffiliated with any particular nation-state, though it made use of the ethereum network." (Reiff, 2021)

A fun example of a DAO was the Constitution DAO that was made in November 2021. Over 5 days, the DAO managed to crowdfund over $47 million in Ethereum. Their plan was to buy the US constitution in the Sotheby Auction then turn it to a non-profit for the DAO holders. It was an interesting idea of a group of regular individual owning shares of the US constitution. However this didn't end well when a fellow billionaire Ken Griffin manage to outbid them in the auction and so the Constitution DAO ended up empty handed.

Aside from ERC-20, there it also ERC-721 which is a standard for Non fungible tokens (NFTs). An NFT is a unique, individual token existing on a blockchain. This tokens can be represented into anything from art, music to even seats for concerts. This non-fungible nature of the tokens means their use cases differ greatly from their fungible counterparts. Each NFT is different and contain identifying information recorded in its smart contract; they are characterized by their unique qualities, as well as authenticity.

Taking the same example from ERC-20, if I have a digital painting and you have a music token, and when we trade we still get different representation of the NFTs not the same like the fungible example.

This is case study I wrote for a research branch of a protocol (under alias Ice Cube) about the most popular NFT collection "Crypto Punks"

"CryptoPunks were one of the first ETH-based NFTs. They are unique digital works of art 24x24 pixel size. There are only 10,000 of them and around 2.8k holders. Due to the different characteristics of each punk, some attributes are more sought after. CryptoPunks in the past have held 69.4% of the entire market volume for NFTs. Totaling $54.17 million out of $78.02 million in the week of 4/14/21-4/20/21.

The CryptoPunks market if recorded from the past 12 months sales ending in April 2021, a little over 8000 sales had resulted in the average sales price of 15.5 ETH ($30,412.40). The total value of all sales is now around 130,000 ETH ($251,620,000) – growing daily. CryptoPunks creators are from the American studio Larva Labs, a two-person team Matt Hall and John Watkinson. Both are Canadian software developers and artists. CryptoPunks were not made with a built-in mechanism to reward their creators, besides scarcity.

Watching the specific CryptoPunk #3011, one of 6039 Male punks, it has a long bidding and transaction history since its creation. First claimed on June 23, 2017, several bids started to range from 0.66 ETH to 14 ETH occurring during the first 2 years. Finally, the punk sold for 23 ETH ($7,843) on October 07, 2020, then quickly selling for 42 ETH ($16,291) on October 12, 2020. The bids began growing due to the number of exclusive accessories the Male punk displays. These accessories include vampire hair, frown, earring, normal beard, pipe, and small shades – Many of these features not many other punks in the set have. The hype around NFTs and CryptoPunks grew substantially in the year following. Thus, resulting in CryptoPunk #3011 selling for 667 ETH ($1.76 million) on April 27, 2021." (Cube, 2021)


(Christie's / Larva Labs)

We can see that Ethereum is becoming its own ecosystem in the blockchain world, because of the creation of DAOs, Dapps and NFTs. It is a multipurpose asset that can be used to create almost anything that you can think off. An example of all this together is a Museum in the Metaverse (just a another term for virtual world), https://oncyber.io/vvd click on the link to experience it.

Regarding with the future of blockchain itself, we can see that Ethereum is shaping the ecosystem we see today with the interesting projects they are doing. There are also a lot of companies focusing their plans more towards this world. Recently, Facebook did a major rebranding to Meta and the payment company Square Inc. turned into Block Inc. Not only that, the mainstream movement of blockchain and crypto even influenced companies to expose their assets into digital assets as well.

MICROSTRATEGY INCORPORATED
CONSOLIDATED BALANCE SHEETS
(in thousands, except per share data)

	September 30, 2021 (unaudited)	December 31, 2020
Assets		
Current assets:		
Cash and cash equivalents	$ 56,975	$ 59,675
Restricted cash	1,149	1,084
Accounts receivable, net	123,748	197,461
Prepaid expenses and other current assets	15,750	14,400
Total current assets	197,622	272,620
Digital assets	2,405,739	1,054,302
Property and equipment, net	38,133	42,975
Right-of-use assets	68,755	73,597
Deposits and other assets	14,857	15,615
Deferred tax assets, net	261,138	6,503
Total assets	$ 2,986,244	$ 1,465,612

(10-q report of Microstrategy)

"

Citation:

Becker, S. (2021, May 11). *Bitcoin hash rate and why it matters*. Https://Www.Sofi.Com/Learn/Content/Bitcoin-Hash-Rate/. https://www.sofi.com/learn/content/bitcoin-hash-rate/

Brown, A. (2021, December 10). *Crypto Investors Wanted To Buy The Constitution. Instead, They Birthed Another Hyped-Up Meme Coin*. Forbes. https://www.forbes.com/sites/abrambrown/2021/12/01/crypto-tokens-people-constitution-dao-ether-redeem-refund/?sh=6fd855a96f3f

Browne, R. (2021, February 23). *Cryptocurrency firms Tether and Bitfinex agree to pay $18.5 million fine to end New York probe*. CNBC. https://www.cnbc.com/2021/02/23/tether-bitfinex-reach-settlement-with-new-york-attorney-general.html

Campesato, J.-B. (n.d.). Prime Numbers, The RSA Algorithm. Concepts in Abstract Mathematics - MAT246H1-S LEC0201/9201 - Winter 2021.

Chitty, T. (2021, December 27). *The Mathematics of Bitcoin — SHA-256 - The Startup*. Medium. https://medium.com/swlh/the-mathematics-of-bitcoin-74ebf6cefbb0

Clark, J. D. D. (2020, July 1). *Demystifying Stablecoins*. July 2020 | Communications of the ACM. https://cacm.acm.org/magazines/2020/7/245698-demystifying-stablecoins/fulltext

Cube, I., & David, B. (2021, September 12). *Tendie research nft guide*. Tendieswap. https://www.tendiebets.org/#/research/tendieresearch-nft-guide

Deshpande, A. (n.d.). *How Blockchain & Machine Learning are disrupting 3 major Industries*. Saviant Consulting. Retrieved December 30, 2021, from https://www.saviantconsulting.com/blog/blockchain-machine-learning-disrupting-major-industries.aspx

Ethereum. (n.d.-a). *ERC-20 Token Standard*. Ethereum.Org. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

Ethereum. (n.d.-b). *Smart contracts*. Ethereum.Org. https://ethereum.org/en/smart-contracts/

Ethereum. (2021, December 2). *ERC-721 Non-Fungible Token Standard*. Ethereum.Org. https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

Froystad, P., & Holm, J. (2016). Blockchain: powering the internet of value. EVRY Labs

Gans, N. (2021, May 13). *Tether (Finally) Releases Breakdown Of Its $42 Billion In Crypto Reserves*. Forbes. https://www.forbes.com/sites/nicholasgans/2021/05/13/tether-releases-breakdown-of-its-reserves/?sh=2f9858011109

Gemini. (2021a, April 28). *What Are Stablecoins? The Global Ecosystem*. https://www.gemini.com/cryptopedia/what-are-stablecoins-list-global-ecosystem#section-crypto-collateralized-stablecoins

Gemini. (2021b, November 30). *What Is a Liquidity Pool? Crypto Market Liquidity*. https://www.gemini.com/cryptopedia/what-is-a-liquidity-pool-crypto-market-liquidity#section-the-role-of-crypto-liquidity-pools-in-de-fi

Guest, G. (2018, January 11). *Cybersecurity via blockchain: the pros and cons*. Technology Record. https://www.technologyrecord.com/Article/cybersecurity-via-blockchain-the-pros-and-cons-62035

Gupta, R. (2021, December 25). *Will OHM Crypto End Up as a Strong Contender of DeFi 2.0?* CryptoTicker. https://cryptoticker.io/en/will-ohm-crypto-end-up-as-a-strong-contender-of-defi-2-0/

Hayes, A. (2021a, August 26). *Is Ethereum More Important Than Bitcoin?* Investopedia. https://www.investopedia.com/articles/investing/032216/ethereum-more-important-bitcoin.asp

Hayes, A. (2021b, November 4). *Blockchain Explained*. Investopedia. https://www.investopedia.com/terms/b/blockchain.asp

Hayes, A. (2021c, November 12). *What Is Stablecoin?* Investopedia. https://www.investopedia.com/terms/s/stablecoin.asp

Hertig, A. (2021, September 22). *What Is DeFi?* CoinDesk. https://www.coindesk.com/learn/what-is-defi/

IBM. (n.d.). *What is blockchain technology?* https://www.ibm.com/ca-fr/topics/what-is-blockchain

IWM. (n.d.). *How Alan Turing Cracked The Enigma Code*. Imperial War Museums. https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

Kastrenakes, J. (2021, May 12). *CryptoPunks NFTs sell at Christie's for $16.9 million*. The Verge. https://www.theverge.com/2021/5/11/22430254/cryptopunks-christies-sale-larva-labs

Lopatto, E. (2021, August 16). *The Tether controversy, explained*. The Verge. https://www.theverge.com/22620464/tether-backing-cryptocurrency-stablecoin

MircoStrategy (2021). Form 10-q. https://www.microstrategy.com/en/investor-relations/financial-documents

Olympus DAO. (n.d.). *Introduction - Olympus*. Olympus. https://docs.olympusdao.finance/main/

Olympus DAO. (n.d.-b). *Olympus DAO | The Decentralized Reserve Currency*. Olympus. https://www.olympusdao.finance/

The Power of Blockchain & Machine Learning in Combination. (2021, November 19). YourTechDiet. https://yourtechdiet.com/blogs/blockchain-machine-learning/

Reiff, N. (2021a, August 5). *What Is ERC-20 and What Does It Mean for Ethereum?* Investopedia. https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

Reiff, N. (2021b, September 24). *Decentralized Autonomous Organization (DAO)*. Investopedia. https://www.investopedia.com/tech/what-dao/

Robinson, M., & B. (2021, October 15). *Cryptocurrency Tether is fined $41 million for lying about reserves*. Fortune. https://fortune.com/2021/10/15/tether-crypto-stablecoin-fined-reserves/

Rooney, K. (2018, June 13). *Much of bitcoin's 2017 boom was market manipulation, research says*. CNBC. https://www.cnbc.com/2018/06/13/much-of-bitcoins-2017-boom-was-market-manipulation-researcher-says.html

Rubio-Licht, N. (2021, December 7). *Meta, Block, Alphabet: Why some companies outgrow their old names*. Protocol. https://www.protocol.com/why-tech-companies-change-names

Wagner, L. (2021a, September 9). *(Very) Basic Intro to Hash Functions (SHA-256, MD5, etc)*. Qvault. https://qvault.io/security/very-basic-intro-to-hash-functions-sha-256-md-5-etc/

Wagner, L. (2021b, November 27). *What is Cryptography? A Complete Overview*. Qvault. https://qvault.io/cryptography/what-is-cryptography/