<https://lameleeadour.com/wp-content/uploads/2018/09/BlockchainCrypto-FabriceBenaut.pdf>

Video :

Blockchain

Cryptoast : [COMPRENDRE LA BLOCKCHAIN EN 7 MINUTES](https://www.youtube.com/watch?v=6uYRN6b5EMU)

[QU'EST-CE QUE LE BITCOIN ? COMMENT CA MARCHE ? EN 5 MN](https://www.youtube.com/watch?v=ItPSIhECknM)





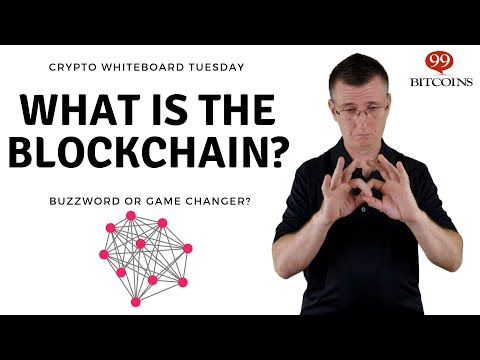
Zone bourse : [Comprendre le Bitcoin (Partie 1)](https://www.youtube.com/watch?v=CCzUaGIg1yw&t=765s)



[Comprendre le Bitcoin (Partie 2)](https://www.youtube.com/watch?v=_CeUHH_GLqw)



[What is Blockchain? Blockchain Technology Explained Simply](https://www.youtube.com/watch?v=2yJqjTiwpxM)



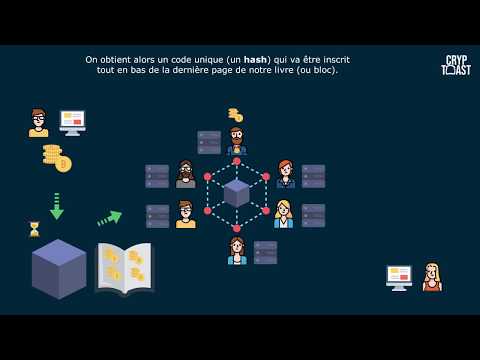
BTC : [Qu'est ce qu'un Halving Day? Rareté et Inflation d'une cryptomonnaie.](https://www.youtube.com/watch?v=TpKo8U3DWU0)



[Qu'est ce que le Bitcoin? Comment fonctionne t-il ? [Simplification]](https://www.youtube.com/watch?v=KizblvpFk9E)



[COMPRENDRE LE BITCOIN EN 4 MINUTES](https://www.youtube.com/watch?v=kQN4upwMlkc)



[Tout savoir sur Bitcoin en 2021 (en 75 minutes seulement)](https://www.youtube.com/watch?v=CYLOhmoHM6I)



ETH :

Cryptoast : [QU'EST-CE QUE L'ETHEREUM ? TOUT COMPRENDRE EN 6 MINUTES](https://www.youtube.com/watch?v=y9MnRJT__9E)



[What is Ethereum? Ethereum 2.0 Explained](https://www.youtube.com/watch?v=dTcojDhr-eE)

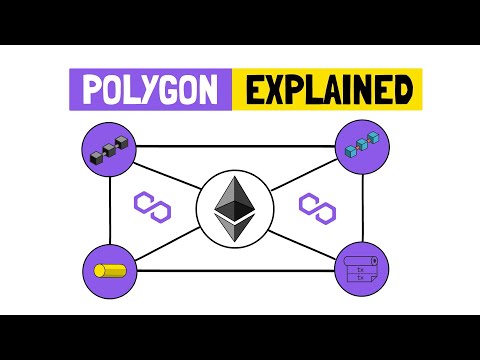


[Ethereum 2021 Explained: What is Ethereum & How it Works (Ultimate Beginner's Guide)](https://www.youtube.com/watch?v=DhoRtGCp4JI)



Layers 2 :

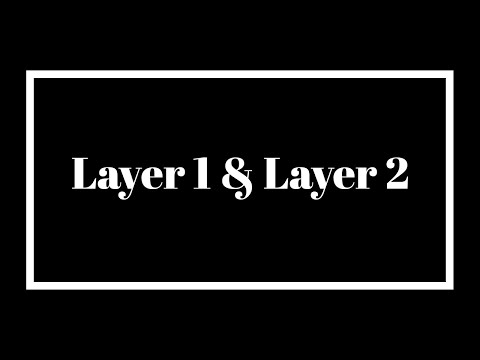
[POLYGON (MATIC) - Ethereum's Internet Of Blockchains Explained - Layer 2](https://www.youtube.com/watch?v=IijtdpAtOt0)



[Comprendre enfin la force des layers 2 et le trilemme de la blockchain!](https://www.youtube.com/watch?v=8Pb-wZAasy0)



[What is Layer 1 & Layer 2?](https://www.youtube.com/watch?v=d7ulxd3R97E)



[What is Layer 1 and 2 in Crypto?](https://www.youtube.com/watch?v=8OQkY3g7e7w)



SOL : [What is Solana? SOL Explained with Animations](https://www.youtube.com/watch?v=1jzROE6EhxM)



[What Is Solana (SOL)?](https://www.youtube.com/watch?v=rqF2vcxkpE4)



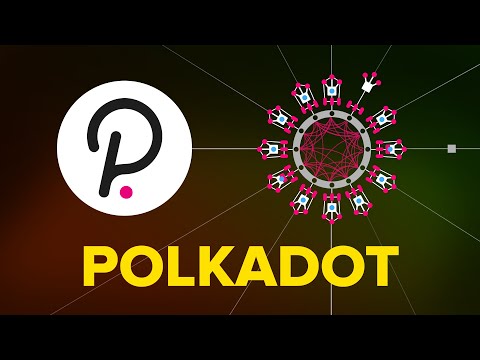
[Solana (SOL) Explained For Beginners 2021](https://www.youtube.com/watch?v=dOHCSs8tMLQ)



[Solana (SOL): Scaling Potential to BLOW Your Mind!! 🤯](https://www.youtube.com/watch?v=FbCUHBhf-rU&list=PLk1ALX7IOH_ln3KuVhuU39wuD_gZyExJb&index=47)



DOT : [What is Polkadot? DOT Explained with Animations](https://www.youtube.com/watch?v=YlAdEQp6ekM)



[Polkadot: the Next Big Thing in Crypto (Polkadot Explained)](https://www.youtube.com/watch?v=QsHbQHjzMuk&t=13s)



<https://medium.com/multi-io/defi-explained-polkadot-c71c21b2221b>

<https://decrypt.co/resources/what-is-polkadot-how-to-buy-it>

<https://www.kraken.com/learn/what-is-polkadot-dot>

Web 3.0 : [What is Web 3.0? (Explained with Animations)](https://www.youtube.com/watch?v=nHhAEkG1y2U)



Stablecoin

[Les STABLECOINS: Quels sont les meilleurs & Comment marchent-ils ?](https://www.youtube.com/watch?v=76u0BBxNcxQ)



[Tout comprendre sur les monnaies stables (ou stablecoins) en 20 minutes !](https://www.youtube.com/watch?v=s1FjaedTh7M)



DEFI

[Au-delà des cryptomonnaies : la Finance Décentralisée](https://www.youtube.com/watch?v=ssQZajKrlWA&t=899s)



[Decentralised Finance: Complete DeFi Overview & Outlook](https://www.youtube.com/watch?v=Vq1bxcoW1jQ&list=PLk1ALX7IOH_npyk1W_88gxTDpTEfZg_Og&index=4)



NFT : [Les NFT : un phénomène artistique et un investissement innovant !](https://www.youtube.com/watch?v=3DQ3qsNRm9g)



POS/POW

[Proof-of-Stake (vs proof-of-work)](https://www.youtube.com/watch?v=M3EFi_POhps)



[Proof of Work vs. Proof of Stake: Beginner's Guide!! 👨‍🏫](https://www.youtube.com/watch?v=08vnE2_cAeQ&list=PLk1ALX7IOH_npyk1W_88gxTDpTEfZg_Og&index=77)



PLAN

**Technology**

Background

We are pleased to be here today to present the most innovative technology of the last few years, which could change the technological world as we know it today: blockchain and cryptocurrencies. Here is the plan that we are going to follow today.

We will talk about the technology of blockchain, cryptocurrencies and we will go further and talk about DeFi, NFT and stablecoins.

Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn’t until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.

In 2010, the first payment with bitcoin was made for 2 pizzas and woth 10 000 bitcoin. Worth today around 6 billion dollar. I hope that pizza were good. In 2011 1 bitcoin was worth 1$ and now around 60 thousand, a huge exponential growth.

Created in 2009 by a person or group of people answering under the name of Satoshi Nakamoto

Linked to the 2008 crisis: need to cut out intermediaries

Goal of the BC = to store digital data in a secure, unforgeable way with a distributed architecture

Vs Fiat => digital + distributed aspect (no more 1 single issuer like a Central Bank)

Blockchain

Let’s begin with an introduction of Hash function : allows from a word / file to obtain a digital fingerprint (hash) = series of characters of fixed length

The digital fingerprint allows to recognize the starting file but unable to trace the fingerprint to the file itself

Probability that 2 objects have the same fingerprint is zero (or almost zero)

What is the Usefulness: compare 2 files between them (just look at the hash and not the file itself)

Ex: widely used for passwords

**What is the relationship between hashing and blockchain?**

BC = blockchain of data

For Bitcoin = chain of transaction blocks

Before being integrated into the chain each block must be validated / calculated by a miner

You can observe the content of a block (hash, data, proof of work etc)

Proof of work (PoW) = calculation that takes a certain amount of time to validate a block (Thomas will explain how it works in a minute)

Why am I explaining this to you? Because hashing is the mainstay of PoW.

When a block is aggregated, it contains multiple transactions as well as information about the previous block. In other words, if someone wanted to change the ledger or make a double spend, he or she would have to change the hash in all previous blocks.

* Secure / unfalsifiable + no intermediaries => great interest in this technology and its use as a currency

**But Blockchain used for many other things:**

E.g.: buying a property requires going to the notary, having huge paperwork / falsification of documents / etc

With a BC: we could do without a notary, have much less paperwork, it would be more secure => can be applied to almost any type of contract

POW/POS

How are crypto created? The main consensus today of creating crypto are called Proof of work and proof of stake.

PoW is Calculation of block hash, like a mathematical puzzle (a little bit more complex but that's the idea). This puzzle is solved by miners and the first one to solve the solution gets the reward, therefore we see huge mining farms with hundreds of computers in the same area, to improve the computing power, improve the hash rate and which enable them to be the first to have the reward which is for Bitcoin network 6.5 BTC per block and 3 ETH for the Ethereum network. Unfortunately, it takes a lot of computing power and electricity and that is why Elon Musk stopped the payment in Bitcoin for its Teslas, because it is not green enough. The most energy is spent on solving the block instead of passing all transaction that is why PoW blockchain are slower than the PoS blockchains

Instead of making a competition between miners and using too much energy to be the first one to mining a new block, a new consensus came, and people are not called miners but validators. To be a validator, you need a certain amount of token to create a node. Node are chosen randomly between all nodes available to validate the next block. The proof of stake seeks to address this issue by attributing mining power to the proportion of coins held by a miner. This way, instead of utilizing energy to answer PoW puzzles, a PoS miner is limited to mining a percentage of transactions that is reflective of their ownership stake. For instance, a miner who owns 3% of the coins available can theoretically mine only 3% of the blocks. This means that the more coin or nodes a person has, the more staking power he has, the more fees reward he gets, the richer he becomes and the more chance he has to be selected as the next validators: this is a problem of PoS.

Here is a slide to resume the two consensuses.

Now lets have a talk on cryptocurrencies. We will first see what a cryptocurrency is, then you will talk about bitcoin and some other main crypto in the market.

**Cryptocurrencies**

What is a Cryptocurrency?

A crypto currency is a digital currency based on blockchain technology, which means that there are almost impossible to counter fit and double spent. Of course, they are not issued by any centralized authorities rendering them theoretically immune to government interference or manipulation. The word “cryptocurrency” is derived from the encryption techniques which are used to secure the network. Cryptocurrencies face criticism for several reasons, including their use for illegal activities, exchange rate volatility, and vulnerabilities of the infrastructure underlying them. However, they also have been praised for their portability, divisibility, inflation resistance, and transparency. The first blockchain-based cryptocurrency was [Bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp), which remains the most popular and most valuable. Today, there are thousands of alternate cryptocurrencies as known as altcoins with various functions and specifications like ETH SOL AVAX POLKADOT. Some of these are clones or [forks](https://www.investopedia.com/terms/h/hard-fork.asp) of Bitcoin, while others are new currencies that were built from scratch.

Balances of crypto asset are kept using public and private "keys" which are long strings of numbers and letters linked through the mathematical [encryption](https://www.investopedia.com/terms/e/encryption.asp) algorithm that creates them. The public key (comparable to a bank account number) serves as the address published to the world and to which others may send Tokens.

The private key (comparable to an ATM PIN) is meant to be a guarded secret and only used to authorize Token transmissions.

**Bitcoin**

What is the Bitcoin and how can BTC be worth something?

Virtual BTC based on nothing? No, based on the trust that investors have in it

Difference with current currencies? 90% virtual currencies

Based on trust? Also, the case with other currencies since the end of the gold standard

BTC would be worthless if the dollar and the euro had all the confidence of people

Currency issued has exploded in recent years and even more so with COVID => Central Banks have opened the floodgates

* Putting a graph money supply

BTC: money creation without human intervention

* We know how many BTC will be created in the future

[Bitcoin mining](https://www.investopedia.com/terms/b/bitcoin-mining.asp) is the process by which Bitcoin is released into circulation. Generally, mining requires solving computationally difficult puzzles to discover a new [block](https://www.investopedia.com/terms/b/block-bitcoin-block.asp), which is added to the blockchain.

Bitcoin mining adds and verifies transaction records across the network.

BTC is created to reward miners

* Put a graph of Supply + Subsidy of BTC (see video 2: <https://www.youtube.com/watch?v=_CeUHH_GLqw>)

Every 210,000 blocks (every 4 years): miners rewards are decreased by 2, this is the halving day

Miners were rewarded 50 BTC per block at its creation

Since May 2020 we are at 6.25

18.5 million BTC created today?

When 21 million have been created: the number of BTC will be fixed

Transaction fees will remunerate miners once this date has passed

If BTC is successful, the number of transactions will make it always profitable to be a miner

Buying and selling BTC: no intermediary in the sense that the transaction is done directly but a marketplace is needed for them to meet (Exchanges: Binance, Coinbase, Kraken)

Coinbase listed this year

As we have seen in class for the classic markets, buying or selling BTC is done in the traditional way with an order book

To be able to buy or sell, the user must have an address attached to a wallet allowing him to store his BTC or more precisely his private key.

It is also possible to gain exposure to crypto currencies through traditional brokers via CFDs or more recently via ETFs.

States can legislate against BTC, prohibit its use as a means of payment, ban the platforms (as in China) but with little success because decentralized network so as long as there are nods of the network BTC cannot be stopped strictly speaking.

To achieve a nefarious act, a bad actor would need to operate 51% of the computing power that makes up Bitcoin. Bitcoin has around 12,809 full nodes, as of early November 2021, and this number is growing, making such an attack quite unlikely.

Bitcoin only has a monetary use, stored value. Just like gold. It was the first blockchain to be implemented, it has enormous historical value. It hardly evolves any more from a software point of view. It will surely remain in proof of work, with a limited quantity of 21 million and especially the current distribution. In short, it's a bit of a consensus in terms of trust.

What about others Cryptocurrencies ?

Is there only bitcoin?

As you might know, bitcoin is not alone, and since BTC is only a value like a digital gold and there is not much or zero project on the Bitcoin blockchain, many developers move towards other blockchain, more secure, fast and with less fees.

The Crypto total, which means the amount of all market cap of all crypto is more than 3 trillion dollars, which is not much for traditional financial, but enormous thinking that cryptocurrencies are only 10 years old.

ETH

Before ETH, crypto currencies were limited in terms of functionality, they were essentially used as digital currencies. Created by Vitalik Buterin in 2013, Ethereum allows developers to create decentralized applications without having to create a new blockchain. This is called the EVM for Ethereum Virtual Machine, it is a decentralized world computer, a supercomputer.

The revolution of ETH is also the release of smart contracts, which start working when certain conditions are met. These are computer programs that just execute what the program has coded, a bit like the functions we wrote during the programming lessons with Roman. For example, in everyday life, to buy a house, you must call a notary, with smart contracts, the notary is not necessary because it is the smart contract that takes his place. You just must read the smart contract, accept it and validate the transaction. Smart contracts dictate the terms of a contract and control its execution within a trusted environment. They make transaction trackable, transparent and permanent.

As I said before, the Ethereum blockchain allows the development of decentralized applications. To put it simply, these are websites where people can play games, exchange NFT or other cryptocurrencies. There are thousands of decentralized applications, and it is surely the future of the internet, to name a few: Sorare, OpenSea, Aave, Uniswap

Moreover, it is possible to create your own crypto currencies on the Ethereum network without having any knowledge about the blockchain. The cryptos created on the ETH network are called ERC20 tokens, there are thousands of them, and the biggest ones are the ones related to DeFi, we will talk about it later.

The main problem of ETH is the number of transactions per second, which is only 15 at that time. Furthermore, to make a transaction, you must pay a fee called gas. This gas varies according to the network occupation and can reach astronomical amounts of a few thousand dollars. So, the ETH network is made for the big wallet and the developers who are in the network for several years and who have in their wallet several hundreds of ETH and who do not have to worry about the gas fees. For a small wallet, there are layers 2 like Polygon, allowing to reduce the price of transactions to fractions of a cent.

The solution for the lack of scalability is the ETH 2.0 update, which will allow to cope with the demands of users of decentralized applications and to be able to accept several thousand transactions per second. ETH 2.0 will also change the network from a proof of work to a proof of stake mechanism, so miners will become validators and will stop using high power and electricity.

Currently there is no photo other blockchains are better. But the fact is that almost the entire ecosystem is on Ethereum. And there have been hundreds of Ethereum killers that have failed before so it's likely to happen again. Eth 2.0 should make up the difference. Also, you should know that the age of a crypto is a very important factor, as is its history. Ethereum was the first Smart contract blockchain.

SOLANA

Solana is an open source blockchain that already uses the mechanism that ETH wants to go to, the proof of stake, but with another feature consensus of time, the proof of history. The creator of SOL thought that the biggest reason for the problem of scalability of bitcoin and Ethereum networks is because the transactions are too low, mainly due to the time taken to order transaction is the right way and came up with a new method called proof of history.

This new consensus does not wait the end of the block to synchronize the network, but each transaction will synchronize the network immediately. Which means that each transaction will represent a period of time and nodes can create the next block without having to coordinate with the entire network first. This mechanism respects the security of the blockchain but also the speed of each transaction because validators don’t need to wait the end of the block.

That is why Solana is the faster blockchain in the world with around 3 new blocks and 50 000 transactions per seconds, 10 times faster than Visa networks. Furthermore, compared to ETH, the fees of each transaction are minimum, for example 1 transaction is around 0.0005$.

The SOL token is mainly used for staking and paying fees but also for DeFi and NFTs. An advantage of Solana is that there is no special requirement to become a validator, remember a validator is a person who helps verify transaction in exchange for rewards. In comparison, you will need 32 ETH to have a node and become a validator on the Ethereum blockchain, which is approximately 150k$.

DOT

Polkadot is a "multi-chain network" that aims to connect different specialized blockchains into a single unified network. It is like a new and improved version of Ethereum, you can make games, use defi and mint NFTs as it was created by one of the founders of Ethereum.

To begin, Polkadot is designed to operate two types of blockchains. A main network, called a relay chain, where transactions are permanent, and user-created networks, called parachains.

The relay chain is the main centered network where transactions are finalized. It provides the shared consensus between the parachains and facilitates cross-chain interoperability. The Polkadot wallets, accounts, and governance are all structured in the Relay Chain. To achieve a greater speed, the relay chain separates the addition of new transactions from the act of validating those transactions. This model allows Polkadot to process over 1,000 transactions per second and cheaper fees compared to Ethereum.

The main feature of Polkadot is Parachains. Parachains can be customized for any number of uses and feed into the main blockchain, so that parachain transactions benefit from the same security of the main chain. It solves the lack of interoperability that other blockchains have because it can connect each blockchain to each other. That is why Polkadot is commonly referred to as a multi-chain network or a layer 0, because it can join networks together, unlike networks like [Bitcoin](https://decrypt.co/crypto-news/bitcoin), which operates on its own.

It uses the Nominated Proof of Stake. Which means that anyone who purchases DOT tokens can use their tokens to propose changes to the network and approve or reject major changes proposed by others. DOT holders can validate the transactions but also nominated a set of validators thanks to their DOT. One more interesting feature is Auction: DOT holders can vote for a project that they want to see live on the Polkadot blockchain.

One of Polkadot’s goals is to fully decentralize the web are users are in control of everything.

**To go further**

DeFi

To simplify what is DeFi, you take the traditional finance system and decentralize them by removing the third-party entity but replacing them with a smart contract. However, the problem is that, to use DeFi, you need to place your money on a platform that creates the smart contract. So DeFi is not completely decentralized, it is more a non-custodial finance, where to don’t need to trust a third party like a bank with your money.

Why using DeFi then?

DeFi enables you to participate in things like loans and fundraising outside of the traditional banking system. The most common things in decentralized finance are Exchanges, Insurance, Lending and Borrowing money to earn interest on the crypto that you hold. And of course, it is not the 0.5% APR of the traditional banks, but up to 20% per year on the most uses platform like AAVE.

We will not talk about collateralization and liquidation because we would need 20 minutes more but basically, everyone can participate in decentralized finance, there is no discrimination regarding your origin or the amount of money available in your bank account, there is no KYC, and you don’t need approval from anyone.

How big is DeFi ?

An interesting website about statistic and metric on defi in defipusle.com Here, you see that there is the equivalent of 104 billion $ and one 2 years ago it was only 600 million dollars. That is a big growth, isn’t it?

What are the disadvantages of DeFi

* First is not easy as it seems to use, you will need to use metamask and be familiar with web 3.0. It is difficult to understand and manipulate, but once you’ve put your money on a DeFi platform, you can do it on another one, it’s just the first time that is hard to understand
* A second disadvantage is risk. Your money is not 100% safe. Hackers or bugs or the platform can take all your money. Many platforms got hacked and millions of dollars were stolen and never gave back. Which means that, one that you can connect to the platform you put money on, and your balance is 0 and you don’t have money anymore because it was hacked.

NFT

**Non-Fungible Token**

Fungible Token => e.g., with Bitcoin: 1 of the very first or the last => interchangeable (they have exactly the same value): you can do the same thing with both

Non-Fungible Token => unique with its own characteristics (each NFT has its own value and cannot be imitated)

NFT = unit that is exchanged through the Blockchain technology

Best known = ERC 721 -> on the Ether blockchain

2017 Cryptokitties (on Ether)

So you're going to tell me something virtual that has value already exists: buying software, an app, a skin in a video game

* How are NFTs different?

Creator could copy and paste and sell it over and over again

NFT = digital scarcity (which did not exist)

Blockchain => creates digital scarcity => when range of NFT issued = unique / can be traced back to who holds it / real token or not?

* Possible thanks to the consistency of the blockchain

**5 main categories of NFTs :**

1/ Collectibles: objects to collect (CryptoKitties)

2/ Metaverses: Ex: NFTs that make you the owner of a piece of land (e.g. Sandbox)

3/ Trading card game: makes you the owner of a card (Ex: gods unchained)

What makes NFTs interesting is that if for example the game developer decides to stop everything, the NFTs created could be used again on another platform if another person decides to develop a similar game

4/ Utilities: provides a service to its owner (e.g. ETH name service => Unstoppable domains in ".crypto", .eth)

5/ Artistic: unique work

Possible use: Trace the authenticity of an object on the internet thanks to the blockchain by associating an NFT with an object

**Which platforms?**

Decentralized platforms that allow the seller to meet buyers (dry sale or auction)

Ex: Rarible / OpenSea

Stablecoins

Stablecoins are cryptocurrencies that are supposed to replicate real world assets, the most used is the US dollar.

In the past, in order to buy Bitcoin, you had to make a transfer from your bank to a platform, wait 3 days for the transfer to arrive on that platform and then buy the Bitcoin. To sell it was the same process but in the opposite direction.

Thanks to stablecoins, like USDT which is the most used stablecoin today, you can directly buy cryptocurrencies while staying on a platform, like Binance. One advantage of using stablecoins is taxes. As we are trading from crypto to crypto, we don't have to pay capital gains tax, which is worth 30% today, however, when you trade from crypto to fiat, which means that you transfer back your money on a bank account, you need to pay the 30% taxes.

How do these cryptocurrencies work to stay stable?

For this, there is the mechanism of collateralization, to ensure that one USDT is equivalent to 1 dollar. The second mechanism is price stabilization to keep the price in balance, even if a whale (a trader with a lot of money) comes and sells his USDT and could make the price drop drastically.

There are 3 main categories of stablecoins:

The first one, the most used, with Tether and Circle, respectively USDT and USDC, uses centralized collateralization, meaning that every time the company wants to offer a USDC or USDT in the blockchain, it must hold a dollar in its bank account.

The second is the collateralization in crypto-currencies, it is the technology used by the Dai. Everything is on chain, for this you must have not 1 USD but for 1.5 USD for 1 Dai to protect from volatility. For example, if BTC drops by 15%, there is an algorithm in the smart contract that will either sell or buy 85 cents of BTC to guarantee the price of one dollar. It is very simplfied but that how it works

The last category of stablecoin is used by the UST on the Terra blockchain, and are called algorithmic stablecoins. Here, the price of a stablecoin is guaranteed by burning, i.e. deleting from the blockchain, $1 of Terra's main crypto, Luna.

What about the risks of your tokens?

Pay attention to the company issuing the stablecoin: make sure they have as many dollars in their safe as the number of stablecoin they are issuing.

Be careful with the smart contract and the algorithm, because if there is a bug, 1 dollar can be worth 50 cents (see the Vai curve)

The risks are also related to the European and American regulators who want its stablecoin issuers to be regulated like a traditional bank.

Pros and cons

### Advantages

Cryptocurrencies hold the promise of making it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or credit card company. These [transfers](https://www.investopedia.com/terms/t/transfer.asp) are instead secured using [public keys](https://www.investopedia.com/terms/p/public-key.asp) and [private keys](https://www.investopedia.com/terms/p/private-key.asp) and different forms of incentive systems, like [Proof of Work](https://www.investopedia.com/terms/p/proof-work.asp) or [Proof of Stake](https://www.investopedia.com/terms/p/proof-stake-pos.asp).

Fund transfers are completed with minimal processing fees, allowing users to avoid the steep fees charged by banks and [financial institutions](https://www.investopedia.com/terms/f/financialinstitution.asp) for [wire transfers,](https://www.investopedia.com/terms/w/wiretransfer.asp) which can take up to 3 days.

### Disadvantages

The semi-anonymous nature of cryptocurrency transactions makes them well-suited for a host of illegal activities, such as [money laundering](https://www.investopedia.com/terms/m/moneylaundering.asp) and [tax evasion](https://www.investopedia.com/terms/t/taxevasion.asp).

The blockchains that use Proof Of Work consensus are also very large consumers of energy.

Crypto assets are also very volatile and are subjects to drops by 50% in only few hours.

Furthermore, in case you failed a transaction, or send your funds to an incorrect address, your funds will be completely lost and not refundable.

A last disadvantage is the interoperability between blockchain. For the moment, you can’t really join two blockchains together like Ethereum and Bitcoin, or you can use bridges, but fees are quite high. Polkadot ecosystem is trying to improve that and make every blockchains connected, which could be a huge improvement.

**Conclusion**

To resume cryptocurrencies, we can say that 2017 was childhood of cryptos with speculation, dark wave, individual traders,

Today we are in the adolescence of crypto currencies market fueled by high finance and WallStreet,

And in 2024 we will see cryptos as adult with a huge adoption by payment services and big companies like GAFAM

In my opinion, we are going to switch to another financial, digital and technological world thanks to blockchain. The technology of blockchain in a kind of revolution that we are just starting. Blockchain, cryptocurrency, Web 3.0 in 2021 might be the Internet is 2000.

I personally don’t think that in the future, there will be lots of different blockchain. Nowadays, we can count more than hundreds of different blockchains, but I guess that in 5 to 10 years, we will only have maximum 5 blockchain including Bitcoin and Ethereum. Some of the blockchain today, will disappear or combine to make one big open source and public blockchain.