

# Cryptocurrency

Szymon Szydlik 5c5

TraPe 2024

Tutrice: Edyta Zenatello





# Table of contents

## **1 Introduction**

- 1.1 What are cryptocurrencies?
- 1.2 The history of cryptocurrencies
- 1.3 Advantages and Disadvantages of cryptocurrencies

## **2 Blockchain technology**

- 2.1 What is a blockchain technology?
- 2.2 Example of a crypto transaction with a blockchain
- 2.3 Different blockchain technology types
- 2.4 Blockchain scalability
- 2.5 Proof-Of-Stake (PoS) vs Proof-Of-Work (PoW)
- 2.6 Popular blockchains

## **3 The first cryptocurrency, Bitcoin**

- 3.1 The creation and important events of Bitcoin
- 3.2 Bitcoin over the years (2008-2023)

## **4 Altcoins**

- 4.1 What are altcoins and what are they good for?
- 4.2 Memecoins

## **5 Crypto scams**

- 5.1 Types of crypto scams
- 5.2 How to avoid crypto scams

## **6 Investing in cryptocurrencies**

- 6.1 Creating a wallet
- 6.2 Buying crypto
- 6.3 Investing

## **7 The future of crypto**

7.1 Possible scenarios

7.2 My prediction

## **8 Game making**

8.1 Planning

8.2 The making

## **9 Conclusion**

## **10 Sources**

# 1. Introduction



## 1.1 What are cryptocurrencies?

Cryptocurrencies, also called 'crypto' are currencies that exist virtually or digitally. They are stored in digital wallets. They are decentralized and normally operate on a technology called blockchain. Unlike traditional currencies, which are controlled by governments or banks, they operate on a network of computers where no one really has control over them. Cryptocurrencies use methods to secure transactions and control the creation of new units. This ensures the privacy of transactions. Most cryptos operate on a public blockchain technology, this way anyone can view transaction histories of cryptocurrencies that operate on that blockchain. Cryptocurrencies only exist in a digital/virtual form and do not exist as banknotes or coins. The first ever cryptocurrency was made in 2009. An anonymous person known as Satoshi Nakamoto published a whitepaper which included Bitcoin. Since the creation of Bitcoin, thousands of cryptocurrencies have emerged, each with their unique features and use cases. Crypto has then become the best way for anonymous transactions. Sadly, many people use cryptocurrencies to pay for illegal items like drugs or anything that is not normally sold.



## 1.2 The history of cryptocurrencies

While Bitcoin is the most well-known cryptocurrency, the concept of digital currencies can be traced back to the 1980s. Various attempts were made to create digital cash systems, but they faced challenges related to centralization and double spending.

What is double spending?

Double spending is a problem when a single digital token can be spent multiple times.

The first ever cryptocurrency was Bitcoin, which was launched in 2009. In 2008, the founder of Bitcoin, Satoshi Nakamoto, introduced a whitepaper that was named "Bitcoin: A Peer-to-Peer electronic cash system". Then in 2009 the first block of the Bitcoin blockchain, known as the Genesis Block, was mined. In the early years, a lot of people were skeptical about Bitcoin. However, it gained interest from technologists and those interested in decentralized systems and digital financial solutions. Bitcoin's value and popularity gradually increased, attracting attention from investors and the media. Inspired by Bitcoin, alternative cryptocurrencies, often referred to as altcoins, were created.

### What are altcoins?

An altcoin is an alternative cryptocurrency to Bitcoin.



Some altcoins include Litecoin, Monero, Solana, and Ethereum. Each of the altcoins introduced different features and improvements to the original Bitcoin protocol. On April 24, 2020, Bitcoin hit 60,000\$. This had a big impact on altcoins, which also hit a big number the time Bitcoin hit that much. People who invested 13\$ in Bitcoin in 2010 would've had 60,000\$ in April 2020. This is because one Bitcoin in 2010 was 13\$. 1 Bitcoin in April 2020 was 60,000\$.

The cryptocurrency space continues to evolve fast, new cryptocurrencies and blockchain technologies are founded regularly, aiming to address scalability, privacy, and much more. Additionally, concepts like stablecoins have emerged, making the future of crypto.

## 1.3 Advantages and Disadvantages of cryptocurrencies

### **Advantages:**

#### Security and privacy

While some cryptocurrencies aren't anonymous, they are pseudonymous, meaning they can mask the identity of users. Even though with proper tools it is possible to trace the owner of transaction addresses, paying with cryptocurrency is always more secure than paying with 'real' money. Cryptocurrencies also use advanced cryptographic techniques to secure transactions, making them highly resistant to fraud and hacking attempts.

#### Accessibility

Cryptocurrencies operate on a decentralized network, that means anyone with an internet connection can participate in transactions and investing, in basically every location on the earth.

#### Transaction fees/costs

Cryptocurrencies often have a low transaction fee.

#### Transaction speed and efficiency

Cryptocurrency transactions are usually processed quickly, eliminating the delays associated with traditional banking systems.

### **Disadvantages:**

#### Volatility

Cryptocurrencies are very volatile, which can lead to unexpected price changes within short periods of time. This can make it risky for investors to predict the price of different cryptos.

#### Lack of regulation

Cryptocurrencies operate in an unregulated environment, which can lead to potential risks, including scams, money laundering, and market manipulation.

#### Complexity

Using and understanding cryptocurrencies requires a certain level of technical knowledge and familiarity with digital wallets, private keys, and blockchain technology, which can be hard to learn for some people.

#### Final transactions

Once a cryptocurrency has been transferred, confirmed, and added to its blockchain, it is almost impossible to redo the action. This can be a problem in the case of accidental or fraud transactions.

#### Limited acceptance

While the acceptance of cryptocurrencies is growing, they are still not widely accepted as a form of payment, limiting their use in everyday transactions.

## 2. Blockchain technology



## 2.1 What is a blockchain technology?

Blockchain technologies are decentralized systems that enable the secure storage and transfer of digital information. At its core, a blockchain is a distributed ledger that records transactions across multiple computers or nodes. These transactions are grouped together in blocks, which then are linked together by cryptographic hashes to form a chain.

Blockchain technologies are most associated with cryptocurrencies, where they serve as the underlying technology. However, a blockchain has also found applications in various other domains other than crypto, such as supply chain management, healthcare, voting systems, intellectual property, and more. By providing a secure and transparent framework for storing and verifying data, blockchain technologies can revolutionize numerous industries and processes.

## 2.2 Example of a crypto transaction with a blockchain

### Step 1:

The person that wants to transfer crypto, creates a transaction with the recipient's crypto wallet and the amount the person wants to send. The transaction also includes other information, such as the transaction fee and some additional data.

### Step 2:

The transaction is broadcasted to the cryptocurrency's network, where it becomes visible to all nodes (computers) in the blockchain network. These computers check if the sender has enough funds to make the transaction.

### Step 3:

Validated transactions are grouped together into blocks. 'Miners', specialized computers in the network, solve a complex mathematical puzzle to add the next block to the blockchain. This process is known as mining.

### Step 4:

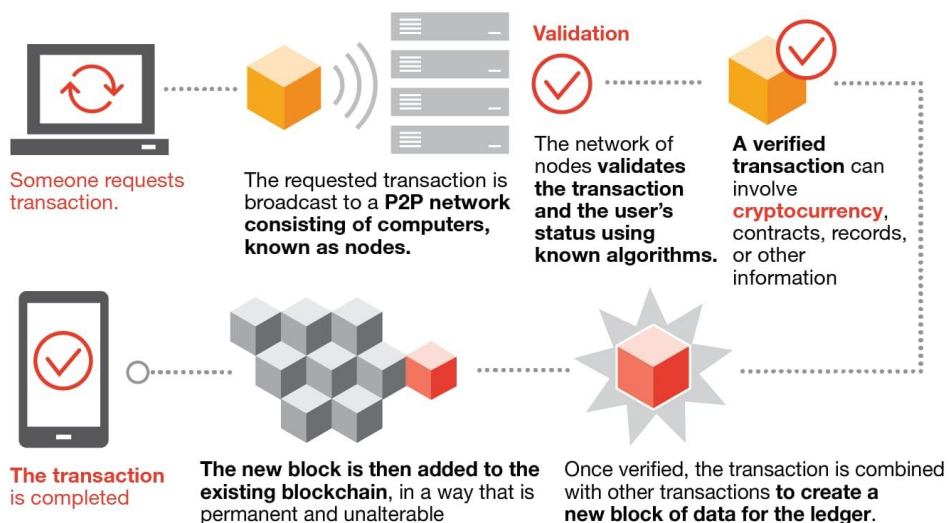
Once a miner solves the puzzle, it broadcasts the newly created block to the network. Other computers verify the block's validity by confirming that the solution is correct and the transactions within the block are legit.

### Step 5:

After the block is added to the blockchain, the transaction is considered confirmed. The confirmation means that it is now part of the history of transactions.

### Step 6:

The recipient gets the transferred cryptocurrency, marking the successful completion of the transaction. Both the sender and the recipient can view this transaction on the blockchain.



This process can take some time, but each cryptocurrency has its own transaction time. For example, a cryptocurrency named Ripple is known for its almost instant transaction time. On the other hand, Bitcoin can take up to 40 minutes to transfer.

## 2.3 Different blockchain technology types

### Public blockchain

A public blockchain is non-restrictive and permissionless, and anyone with internet access can sign on to a blockchain platform to become an authorized node. This user can access current and past records and conduct mining activities, the complex computations used to verify transactions and add them to the ledger. No valid record or transaction can be changed/edited in the network, but anyone can see the transactions, find bugs, or propose changes because the source code is usually an open source. But if the blockchain is public, it doesn't mean it is not safe. Blockchains are secured very well.

### Private blockchain

A private blockchain is a blockchain that works in a restrictive environment like a closed network, or the one that is under the control of a single entity. While it operates like a public blockchain, this type of blockchain is on a much smaller scale. Instead of just anyone being able to join and provide computing power, private blockchains typically are operated in a small network inside a company or organization. This means, unlike public blockchains, not everyone can fix bugs or see transactions.

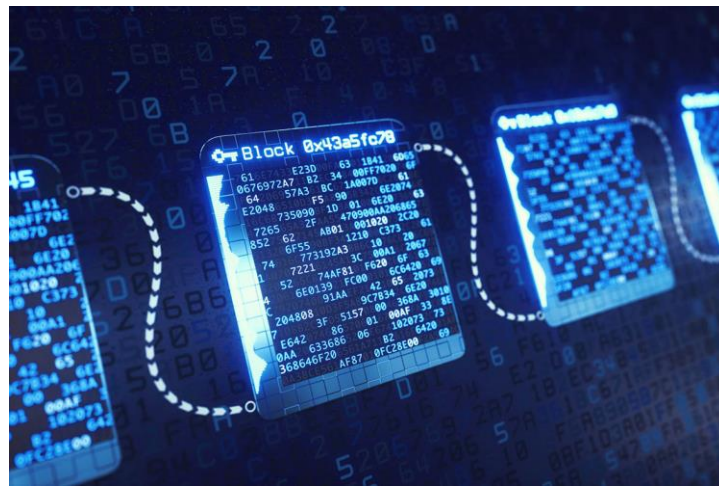
### Hybrid blockchain

Sometimes, organizations or companies want the best of both worlds, and choose to use a hybrid blockchain, which is a type of blockchain technology that combines elements of both private and public blockchains. It lets organizations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored in the blockchain, and what data will be opened up publicly. Typically, transactions and records in a hybrid blockchain are not made public but can be verified when needed.

### Consortium blockchain

The fourth type of a blockchain, consortium blockchain, also known as a federated blockchain, is similar to a hybrid blockchain. But it is different because multiple organizational members collaborate on a decentralized network. Essentially, a consortium blockchain is a private blockchain with limited access to a particular

group, eliminating the risks that come with just one entity controlling the network on a private blockchain.



## 2.4 Blockchain scalability

Scalability is a critical challenge for blockchain technology as it aims to handle a larger number of transactions and users while maintaining efficiency. Here are some techniques blockchains use to overcome that challenge:

### Layered solutions

Many blockchain platforms employ layered solutions to improve scalability. These solutions, such as off-chain channels and sidechains, enable transactions to be controlled off the main blockchain, reducing congestion and increasing throughput.

### 'Sharding'

Sharding involves dividing/splitting the blockchain network into smaller partitions called shards, each capable of processing a subset of transactions. This allows for parallel processing of transactions, strongly enhancing scalability. However, maintaining consensus across shards and ensuring data integrity are not easy challenges.

### Consensus mechanisms

Traditional blockchains like Bitcoin and Ethereum rely on consensus mechanisms such as Proof-of-Work (PoW), which require large computational resources. As a result, these networks face scalability issues. Alternative consensus mechanisms like Proof-of-Stake (PoS) and Delegated Proof-of-Stake (DPoS) have higher transaction throughput and energy efficiency, addressing scalability concerns.

## 2.5 Proof-of-Stake (PoS) vs Proof-of-Work (PoW)

Decentralized cryptocurrency networks need to make sure that no one spends the same cash twice without a central authority like Stripe or PayPal in the middle. To do this, networks use something called a “consensus mechanism,” which is a system that allows all the computers in a crypto network to agree about which transactions are legit.



### What is Proof-of-Work (PoW)?

Proof-of-Work is the original crypto consensus mechanism, which was first used by Bitcoin. Proof-of-Work blockchains are secured and verified by virtual miners around the world racing to be the first to solve a very complex math puzzle. The winner gets to update the blockchain with the latest verified transactions and is rewarded by the network with a predetermined amount of crypto. This mechanism is called ‘Proof-of-Work’ because it checks if the miner has solved the puzzle, and if it proves that the puzzle is solved, the miner receives an amount of crypto. It is like you have to prove that you have done a task to get paid.

## What is Proof-of-Stake (PoS)?

Proof-of-Stake (PoS) is an alternative consensus algorithm. Unlike Proof-of-Work (PoW) which relies on computational work and energy consumption, PoS selects block validators based on the amount of cryptocurrency they hold and 'stake' in the network. In PoS nodes are referred to as validators not miners. Validators are selected based on the cryptocurrency they own and are willing to stake. The more cryptocurrency they have and stake, the higher their chances of being chosen as validators. Validators take turns validating new blocks. Their job is to verify transactions and add them to the blockchain. They need to act 'serious' because they have their own crypto staked. If they don't do their job as they should, they could lose some of their staked crypto.

## Comparison: Proof-of-Stake vs Proof-of-Work

	Proof-of-Stake	Proof-of-Work
Energy consumption	PoS consumes way less energy compared to PoW. It doesn't require intensive computational work or mining hardware	PoW requires a big amount of power because it solves very complex math puzzles that require a lot of computational work. In 2018, the Bitcoin network (PoW) alone used <b>22 Terawatt-hours</b> of energy
Security (51% attacks)	The hacker would need to own 51% of all the cryptocurrency on the network, which is basically impossible	The hacker would need to have a computer more powerful than 51% of the network to add a hacked block,
Fairness	PoS is considered unfair because the validators with the most staked crypto have a higher chance to be chosen to validate a block	PoW is often regarded as a fairer consensus algorithm as it allows participants to compete for block rewards based on their computational resources

In my opinion, I find that Proof-of-Stake is a better option. It is faster in general, and more secure for certain cyberattacks. It is also much more energy efficient than PoW.

## 2.6 Popular blockchains

### Ethereum

The fastest blockchain is named after the cryptocurrency Ethereum. Ethereum is completely decentralized and boasts complete support for smart contracts. The Ethereum blockchain can process up to 20,000 TPS (Transactions per second). Since 2022, the Ethereum blockchain has switched to PoS.



### Avalanche

Avalanche is a blockchain platform that aims to provide a scalable, decentralized, and good infrastructure for building decentralized applications and financial systems. Avalanche can process up to 4,500 TPS.



## Cardano

This proof-of-stake blockchain says it is the first founded on peer-reviewed research. Use cases include verifying credentials such as diplomas, establishing provenances to prevent the online sale of fake luxury goods and supporting stakeholders along the food-production chain, from farmers to retailers. The Cardano blockchain can process up to 1,000 TPS.



## Solana

Solana offers the ability to create “scalable, user-friendly apps” with its platform, and also says it’s one of the fastest blockchains in the world, with 400 millisecond block times. It is also decently secure, low-cost (about 0.01 \$ per transaction) and resistant to censorship because the network is spread over thousands of independent nodes.



Of course, there are many more blockchains out there that are good for their own different purposes.

### 3. The first cryptocurrency, Bitcoin



### 3.1 The creation and important events of Bitcoin

The first ever cryptocurrency was Bitcoin, which was launched in 2009. It was made by an anonymous person called “Satoshi Nakamoto”. To this day, nothing is really known about this mysterious person. As said before, the idea of Bitcoin was to create a digital cash system that is fast, reliable, and not under control by authorities. Bitcoin was originally designed as a medium of exchange but is now regarded as a store of value.

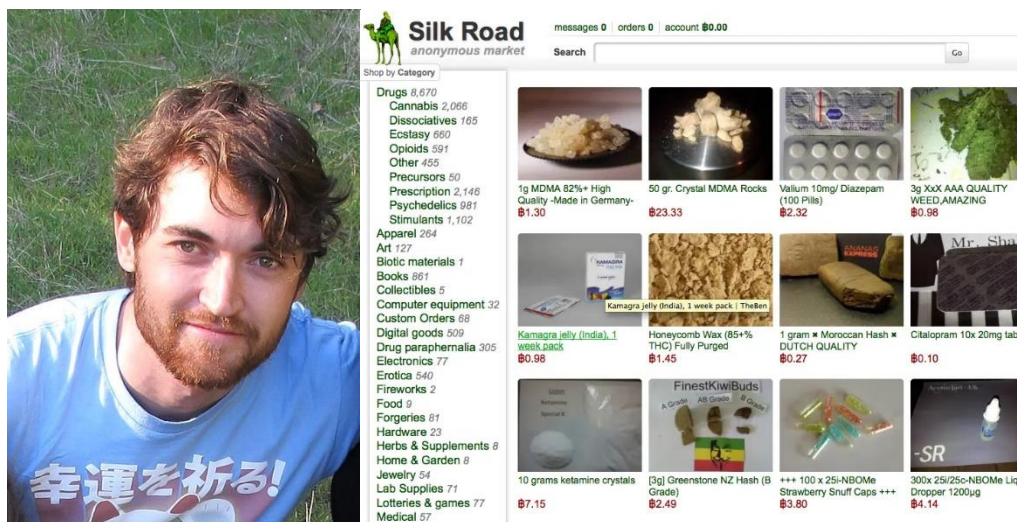
#### What is a medium of exchange?

A medium of exchange is something that is used to buy/sell something. For example, money.

#### What is a store of value?

A store of value is an item that gains value over time. For example, houses, land, rare materials, crypto... (A store of value’s value can also decrease overtime) 2010, Laslo Hanyecz made the first real-world crypto payment by buying a pizza with 10000 Bitcoins. That amount would be over 200 million dollars in 2023! However, in 2010, 10000 bitcoins were worth only a few dollars.

In 2011, the Silk Road marketplace went live. Silk Road would be a hotspot for buying and selling illegal items like drugs and stolen goods. It was one of the first real-world applications where you could pay with Bitcoin. In 2013 the website was shut down by the FBI and arrested the person behind it, Ross Ulbricht.



Silk Road 2.0 was released the month after, run by former Silk Road administrators. It was taken down the following year.

In 2013, a person named Davinci Jeremie uploaded a YouTube video titled “Bitcoin Update - just buy \$1 worth of bitcoin please!”. In the video he explained how it would be smart to buy 1 dollar worth of bitcoin. Some people listened, some did not. If they had bought 1 dollar of Bitcoin in early 2013 (When 1 BTC was about 13 dollars), they would have had about 5600 dollars in November 2021. Video: <https://www.youtube.com/watch?v=Cw29h7LhEuE>



The first Bitcoin ATM was also built in 2013 in Vancouver, Canada. Since then, Bitcoin ATMs became more common with thousands worldwide.

In 2014, Mt. Gox, one of the largest Bitcoin exchanges, filed for bankruptcy. The exchange claimed that it lost 850000 Bitcoins, worth about 400 million dollars at the time, due to a hacking attack.

As of November 2021, 9 countries have banned Bitcoin and other cryptos. These countries are China, Afghanistan, Nepal, Bangladesh, Morocco, Algeria, Egypt and Bolivia. The cause of crypto bans in these countries are mostly because of the lack of government control over the digital currency, or fears of money laundering. 44 other countries have partially banned Bitcoin/crypto. (For example, trading is allowed but transactions with crypto are banned.)

Overall, Bitcoin is becoming more popular day by day. As of 2023, 75% of retailers are planning to accept Bitcoin and other cryptocurrencies in about 2-3 years.

## 3.2 Bitcoin over the years (2008-2023)

### 2008

The bitcoin.org domain was registered.

### January 3, 2009

The Bitcoin network went live with the creation of the first block, known as the Genesis Block. This marked the official release of Bitcoin.

Bitcoin introduced several groundbreaking concepts and technologies. It utilized a decentralized peer-to-peer network known as the blockchain, to log and verify transactions.

### May 22, 2010

Laszlo Hanyecz made the first real-world transaction by buying two pizzas in Jacksonville Florida for 10,000 Bitcoins.

### December 31, 2010

One Bitcoin is worth about 0.09 \$.

### 2011

One Bitcoin is now worth about 1 \$.

### November 29, 2013

Bitcoin skyrockets and reaches about 1,240 \$.

### April 11, 2014

Bitcoin drops to 340 \$ because of the Cypriot financial crisis.

### May 20, 2017

Bitcoin reaches 2,000 \$ for the first time in history.

### December 17, 2017

Bitcoin absolutely skyrockets, reaching 19,000 \$.

### December 22, 2017

Bitcoin lost one third of its value in 24 hours, dropping below 14,000 \$.

### February 5, 2018

Bitcoin's price dropped by 50% in about 15 days, falling below 7,000 \$.

### October 31, 2018

This date marks the 10<sup>th</sup> anniversary of Bitcoin. The price stays steady at 6,300 \$.

### July 1, 2019

1 Bitcoin is now about 10,000 \$.

### November 30, 2020

Bitcoin's price goes up to 19,000 \$.

### February 8, 2021

Bitcoin absolutely skyrockets yet again, reaching 44,200 \$. The cause of this was because Elon Musk's investments into Bitcoin, including acceptance of payment.

### April 14, 2021

This marks the 'golden day' of Bitcoin. For the first time ever, Bitcoin reaches a insane amount of 64,800 \$. People that would have invested 100\$ (About 1,000 BTC) into Bitcoin in 2010, would have had 64 million \$ at this time.

### May 12, 2022

Following the Terra-LUNA crash in May 2022, Bitcoin retreated to its lowest level since December 2020, 25,000 \$.

### March 17, 2023

One Bitcoin is worth about 26,500 \$.

### July, 2023

Bitcoin's price stays steady at 28,000-30,000\$

## 4. Altcoins



## 4.1 What are altcoins and what are they good for?

Altcoins refer to any other cryptocurrency other than Bitcoin. They often serve different purposes, some are more secure, some are faster. This makes them suitable for many use cases:

### Diversification

Altcoins allow investors to diversify their cryptocurrency beyond Bitcoin. This helps lowering risk, as Altcoins have different price movements and market dynamics.

### Innovation

Altcoins often introduce features that Bitcoin does not have.

### Specific use cases

Some Altcoins are designed for specific use cases.

### Privacy

Altcoins like Monero and ZCash prioritize security and privacy. They offer even more secure transaction encryptions, making them a hotspot for people that value privacy.

### Scalability and speed

Altcoins like Litecoin and Bitcoin Cash have faster transaction times than the original crypto, Bitcoin. They are also optimized more.

### Investment opportunities

Altcoins can have investment opportunities that have potentially higher returns.

It is important to know, while Altcoins offer a lot of great benefits, they also come with their own risks.

## 4.2 Memecoins

In crypto, Memecoins are cryptos that were made and named after a meme. For example, the well-known crypto named Dogecoin, which was made by two software engineers Billy Markus and Jackson Palmer.



These coins usually have no utility, just trading value. They have a very low value, usually  $\sim 0.00001$  dollars or even less. The main thing about Memecoins is that they can get very popular and gain an absurd increase in value just overnight, just from social media buzz. This also means that Memecoins are extremely volatile. An investor invested 27 dollars in a Memecoin named “Pepe coin” and got a 340000x return. That’s more than 1 million dollars from a 27 dollar investment. However, Memecoins can be manipulated to enrich insiders. South Korea’s Virtual Asset User Protection bill penalizes market manipulation and unfair practices. Europe’s new Markets in Crypto-Assets legislation compels influencers to disclose any compensation they receive from projects they promote.

## 5. Crypto scams



## 5.1 Types of crypto scams

A scam is often referred to as a fraud. It is an “illegal trick”. Scams succeed because they often seem very believable. In crypto scams are quite common, especially since everything is anonymous. As a result, the person behind the scam can get away with it easily.

Here are the most common crypto scams:

### Phishing scams

Phishing scams are by far the most common scam on the internet. According to the FBI, over 300000 people fell for phishing scams in 2021. This resulted in over 40 million dollars being stolen. Phishing scams are very easy to fall for, and surprisingly easy to make. Usually, scammers create an exact copy of a website, for example Binance (one of the biggest crypto exchange companies). You think this is the real website, but when you log in with your details, they will be sent to the scammers. This information usually is your crypto wallet key or your login details. One popular tool is called “Zphisher”, which is easy to download and use.



In this tool, all you must do is select which site you want to make a replica of and voila – you have made your phishing site.

### Blackmail scams

Blackmailing is when a person demands money or another benefit from someone in return for not revealing damaging information about them. In this scam, scammers send blackmail emails. In such emails, scammers claim to have a record of illegal websites (ex. child pornography websites/black market websites) that the person has visited and threaten to expose this information to authorities unless given the person's crypto wallet keys.

### Investment opportunity scams

Scammers make misleading websites offering "guaranteed returns" for investing in their altcoins or other setups for which investors invest very large sums of money for even larger "guaranteed" results. Then, investors try to get their money out and find out they cannot.

### Online crypto gambling sites

Some people may not consider this a scam, but I do. Since crypto is unregulated, it is difficult to control if these gambling sites run their business legitimate. Because of this, some of these gambling sites may be rigged, meaning they are very unfair. There also have been cases of crypto gambling sites sending people's withdrawals to wrong crypto addresses, or not letting them withdraw at all.

### Rug pulls

A rug pull occurs when scammers raise money or crypto to fund a project and then suddenly remove all of the liquidity and disappear. The project is abandoned, and investors lose everything that they have contributed.

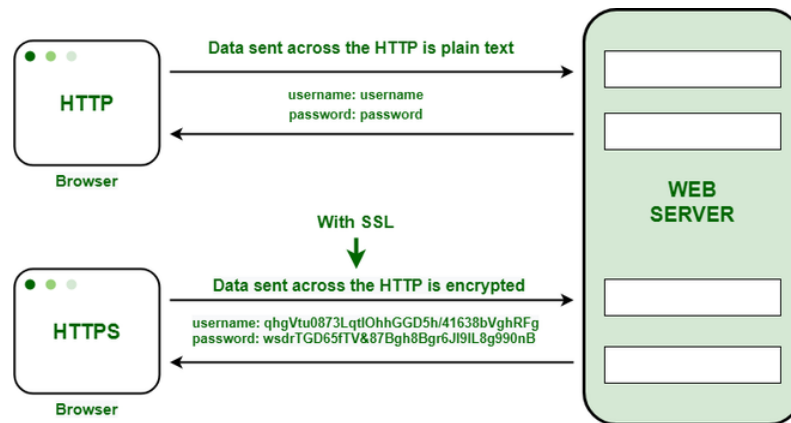
### Identity fraud

Hackers/scammers compromise social media accounts and post fake stories on them. Ex. "I just invested ... in this crypto and got a huge return!". Since hackers aim to compromise big accounts, like celebrities etc. it may seem very believable to people. I mean, your favorite celebrity wouldn't scam you, would they?

## 5.2 How to avoid crypto scams

### Phishing scams

Avoiding phishing scams is easy, but a lot of people still fall for it. All you must do is check if the site's link is suspicious. The first method to do that is to check if the site is secure. If a site starts with http instead of https, it is better to avoid it. This is because data sent from a http website is not encrypted.



The second method to check if the site is not a replica, is verifying the link. Usually, phishing sites may have a modified link. For example, Binance's link is "https://binance.com". Scammers try to create a link that looks almost the same, which means you won't notice it unless you take a closer look. For example, "https://blnance.com" or "https://binacne.com". Again, to avoid phishing sites, just verify the link. Still, if you think a site is suspicious, it is better to leave it.

### Blackmail scams

This scam may be believable to people that have already visited such websites before. If you haven't, it's easy to tell this is a scam. Most of the time, real blackmail claims won't be sent by email.

### Investment opportunity scams

There is a very easy way to avoid this scam: if something sounds too good to be true – 99% of the time, it is. No investment has "guaranteed results".

### Online crypto gambling sites

Again, some people may not consider this a scam, but I believe it is better not to go on such sites, you will end up losing your money either way, it is gambling.

### Rug pulls

I don't know how to specifically avoid this one. Just think twice before investing/funding a project.

### Identity fraud

Make research if the account is compromised. A celebrity may have an account on another platform where they posted that their main account has been hacked. If a celebrity has never been really interested in crypto, why would they talk about it all of a sudden? Their account is most likely compromised if they do something like that.

## 6. Investing in cryptocurrencies



## 6.1 Creating a wallet

The first step that is required to sell or buy crypto is owning a crypto wallet. Thus we need to create it. There are 3 wallet types to choose from:

### Hot wallet

A hot wallet is the most popular wallet type. To create a hot wallet, all that is needed to do is download a wallet provider, for example Trust wallet, and make a new wallet. You can download a hot wallet on your phone and PC.

### Cold wallet

A cold wallet is a wallet that does not need internet connection to store your cryptocurrencies. The most popular type of cold wallet is a hardware wallet, which mostly takes form of a USB stick.



Cold wallets are considered more secure.

### Paper wallet

A paper wallet is a form of a cold wallet. It is the most secure wallet because it is stored physically on a piece of paper. It is created on a site that generates keys. The site works without an internet connection, and once the keys are generated you'll be able to print them out. The next step would be to go on a site like <https://blockchain.info> and import your wallet by putting your key and address.

## 6.2 Buying crypto

To buy crypto, you must be over 18 because most companies that sell crypto ask for ID verification. Different sellers have different exchange rates, you want to find a seller with the lowest buy fee/exchange rate. Coinbase and Binance often have the cheapest fees and exchange rates. Alternatively, you could find a person that would give you crypto in exchange for cash.

## 6.3 Investing

Again, investing in crypto is risky due to it being very volatile. Therefore, guaranteeing any profits is impossible. One of the best times to buy crypto is when events happen that guarantee the rise of a cryptocurrency. For example, when war breaks out people start investing in companies that make war equipment. The same is for crypto you need to wait for events to happen that will raise the price. Another good time to buy crypto is during a bear market.

### Bear market

A bear market is when a cryptocurrency's price drops drastically in a short time. This is the best time to buy crypto due to the coins price being very cheap. 90% of the time, investing during a bear market will return profits. If this goes to plan, investors will make big profits during a bull market.

### Bull market

The exact opposite of a bear market. A bull market is when a crypto's price rises quickly.

## 7. The future of crypto



## 7.1 Possible scenarios

### Real-life payments

Possibly in the future, more and more real-life stores will start accepting crypto as payment. This way people could buy groceries when paying with crypto. In my opinion, this won't really happen because we normalized paying with "real" currencies. You would also never really know how much money you have due to crypto being very volatile.

### Countries banning crypto

It is possible that countries ban crypto completely, due to the anonymity of the transactions. Some countries also consider crypto as gambling, that may also be the cause.

### Intergration with traditional finance

Cryptocurrencies and blockchain technology could become integrated with traditional financial systems, leading to the emergence of hybrid financial services that offer the benefits of both sides. This could include tokenized assets, blockchain-based settlement systems, and decentralized finance (DeFi) platforms.

### Market Consolidation

A period of market consolidation could occur, with many smaller cryptocurrencies and projects failing or merging, while larger and more established projects dominate the landscape. This could lead to a more mature and stable cryptocurrency market.

## 7.2 My Prediction

I think that crypto will be the future of "anonymous" payments. If cash becomes used less, crypto will serve as the next "anonymous" payment method. I also think that more and more people will start using crypto. Maybe there will even be real-life payment with crypto.

## 8. Game making



## 8.1 Planning

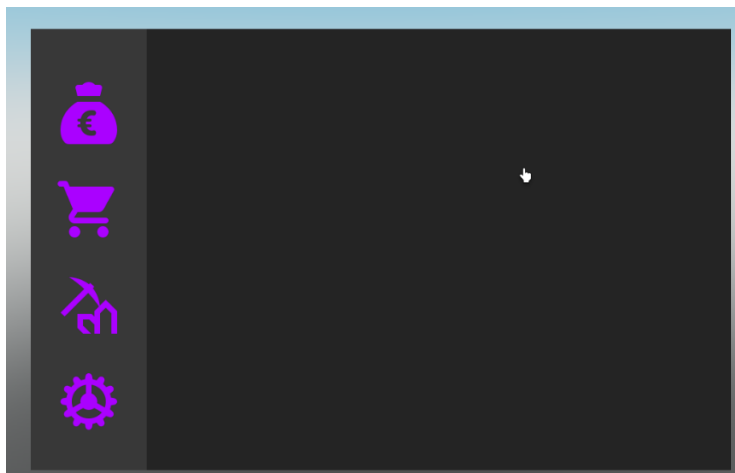
As a practical part of my TraPe, I decided to design a game about crypto trading. The basic rules are as follows:

- > The player has a balance
- > The player needs to buy / sell crypto to increase their balance and make profits
- > Losses can happen due to the game being random
- > With the balance the player can buy crypto mining machines and other accessories
- > The goal is to accumulate as much cryptocurrency as possible

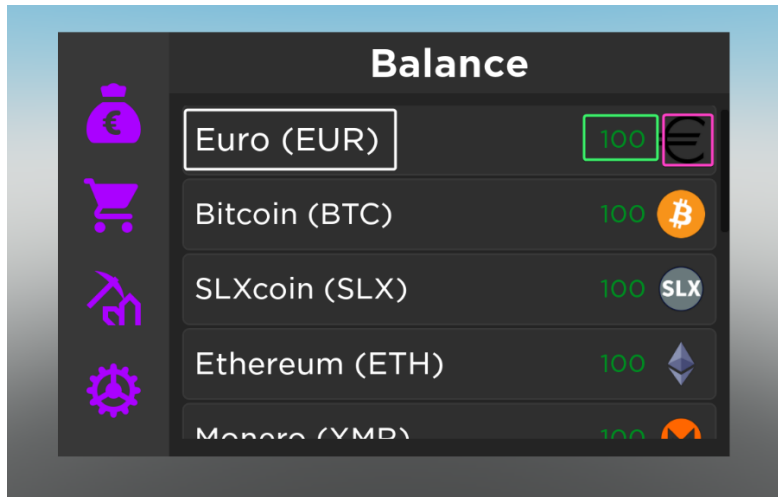
For the programming language I used Lua, for the game engine - Roblox Studio and for the code editor - VScode. I chose Roblox Studio because I have previous experience with it and while also being able to use Unity or CryEngine, I prefer using RStudio due to various reasons. For example, it is much easier to create UI with it.

## 8.2 The Making

I started by making a new project and making the main UI design for the game. I decided to go with a modern look. Then, I added some icons on the right since I thought it would look better than plain text. These would be used to navigate between tabs/pages.



Next, I wanted to design the first page first, which would be the “Balance” page.

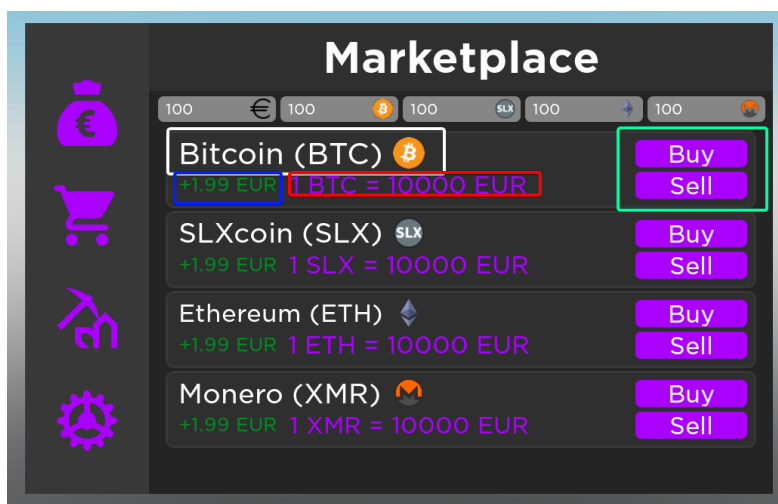


In the balance page I added all currencies I wanted to add to my game and the euro balance which is the primary balance. I will add 4 cryptos to the game:

- > Bitcoin
- > SLXcoin (custom made crypto)
- > Ethereum
- > Monero

The text in the white box is the currency’s name, the green box shows the balance, and the pink box shows the image for the currency.

Next, I needed to design the shop – a place where you can buy/sell crypto.



Here I added all the cryptos. I also added a little overview of a player's balances, so they don't need to switch tabs so often. The white box shows a crypto's name and icon, in the green box there is the buy and sell button. The blue box shows how much a crypto has increased/decreased in value and the red box shows the current value of the crypto.

Before designing other pages, I made the crypto buying/selling functional. I also made the balances and the crypto values work.

As this game is singleplayer, I will rely only on the client, there is no point in using server-side code.

```
1  local Interface = script.Parent.Background
2  local Buttons = Interface.SideFrame.Buttons
3  local Balance = Interface.Balance
4  local Marketplace = Interface.Marketplace
5
6  ▼ local Balances = {
7      ["Euro"] = 0;
8      ["Bitcoin"] = 0;
9      ["SLXcoin"] = 0;
10     ["Ethereum"] = 0;
11     ["Monero"] = 0;
12 }
```

I started by putting the balances in a table and making variables.

```
14 ▼ local Values = {
15     ["Bitcoin"] = 0;
16     ["SLXcoin"] = 0;
17     ["Ethereum"] = 0;
18     ["Monero"] = 0;
19 }
20
21 ▼ local LastValues = {
22     ["Bitcoin"] = 0;
23     ["SLXcoin"] = 0;
24     ["Ethereum"] = 0;
25     ["Monero"] = 0;
26 }
27
28 Balances.Euro = 500;
29
30 Values.Bitcoin = math.random(7000,10000)
31 Values.SLXcoin = math.random(500,700)
32 Values.Ethereum = math.random(2000,4000)
33 Values.Monero = math.random(100,500)
34
35 function RandomizeValue(CurrentPrice, IncMin, IncMax, LastPrice)
36     local R1 = math.random(1,2)
37     if R1 == 1 then
38         return CurrentPrice + math.random(IncMin, IncMax)/(LastPrice/3)
39     elseif R1 == 2 then
40         return CurrentPrice - math.random(IncMin, IncMax)/(LastPrice/3)
41     end
42 end
```

Then, I made 2 new tables which store the Value of the crypto and the last price. I also set the Euro and Crypto values to a random number in the start, so the player has something to start with. Next, I made a function which will randomize the crypto's value according to its last price and via pure randomness.

```

43  ▼ coroutine.wrap(function()
44  ▼    while wait(1) do
45      --// Randomize BTC
46      LastValues.Bitcoin = Values.Bitcoin
47      local x = RandomizeValue(Values.Bitcoin,100,400,LastValues.Bitcoin)
48      print(x)
49
50
51    end
52  end) ()

```

To test the randomizer, I wrote a coroutine loop, which randomizes the crypto's value every second. Afterwards, I corrected these 2 lines that returned the randomized value, and changed the way they work due to the other method altering the value too slowly to my liking.

```

return CurrentPrice + math.random(IncMin,IncMax) + (LastPrice/5)
if R1 == 2 then
return CurrentPrice - math.random(IncMin,IncMax) - (LastPrice/5)

```

Next, I added the rest of the cryptos to the loop

```

43  ▼ coroutine.wrap(function()
44  ▼    while wait(1) do
45      --// Randomize BTC
46      LastValues.Bitcoin = Values.Bitcoin
47      local BTC = RandomizeValue(Values.Bitcoin,200,500,LastValues.Bitcoin)
48      print("Current BTC value: "..BTC)
49      LastValues.Bitcoin = Values.Bitcoin
50      --// Randomize SLX
51      LastValues.SLXcoin = Values.SLXcoin
52      local SLX = RandomizeValue(Values.SLXcoin,150,320,LastValues.SLXcoin)
53      print("Current SLX value: "..SLX)
54      LastValues.SLXcoin = Values.SLXcoin
55      --// Randomize ETH
56      LastValues.Ethereum = Values.Ethereum
57      local ETH = RandomizeValue(Values.Ethereum,400,600,LastValues.Ethereum)
58      print("Current ETH value: "..ETH)
59      LastValues.Ethereum = Values.Ethereum
60      --// Randomize XMR
61      LastValues.Monero = Values.Monero
62      local XMR = RandomizeValue(Values.Monero,50,100,LastValues.Monero)
63      print("Current XMR value: "..XMR)
64      LastValues.Monero = Values.Monero
65    end
66  end) ()

```

Afterwards, I ran the script again and tested if the values would all randomize.

```

15:57:57 -- Current BTC value: 11877.8
15:57:57 -- Current SLX value: 940.2
15:57:57 -- Current ETH value: 3743.4
15:57:57 -- Current XMR value: 563.2
15:57:57 -- Current BTC value: 7258.2
15:57:57 -- Current SLX value: 239.8
15:57:57 -- Current ETH value: 3729.4
15:57:57 -- Current XMR value: 556.2
15:57:58 -- Current BTC value: 11867.8
15:57:58 -- Current SLX value: 245.8
15:57:58 -- Current ETH value: 1622.6
15:57:58 -- Current XMR value: 239.8
15:57:59 -- Current BTC value: 11841.8
15:57:59 -- Current SLX value: 907.2
15:57:59 -- Current ETH value: 3884.4
15:57:59 -- Current XMR value: 534.2

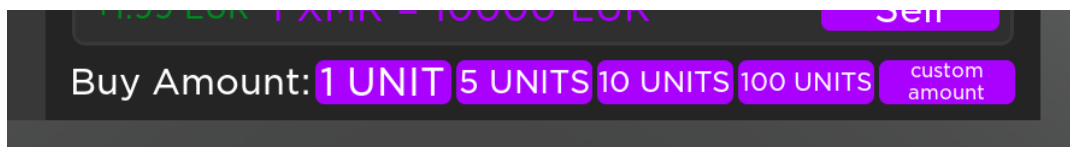
```

It worked well, but I made another change to the randomizer code; I fixed a bug where a crypto's value would drop under 0 EUR.

```
40     local Value, Inc = CurrentPrice - math.random(IncMin, IncMax) - (LastPrice/5), false
41     if Value < 0 then
42         return CurrentPrice + math.random(IncMin, IncMax) + (LastPrice/5), true
43     else
44         return Value, Inc
45     end
46 end
47 end
```

I also made the crypto's value display on the shop page.

Next, I made the buying/selling functional.



First, I added some buttons where you can change the amount of crypto you're buying.

```
118 for _, BA in pairs(Marketplace.BuyAmt:GetChildren()) do
119     if BA:IsA("TextButton") then
120         if BA.Name == "B1" then
121             BUY_AMT = 1
122         elseif BA.Name == "B5" then
123             BUY_AMT = 5
124         elseif BA.Name == "B10" then
125             BUY_AMT = 10
126         elseif BA.Name == "B100" then
127             BUY_AMT = 100
128         end
129     elseif BA:IsA("TextBox") then
130         BA.FocusLost:Connect(function()
131             BUY_AMT = BA.Text
132         end)
133     end
134 end
```

Then, I made the buttons functional. Next, I made the buying/selling script.

```
151 for _, Crypto in pairs(Marketplace.Cryptos:GetChildren()) do
152     if Crypto:IsA("Frame") and Crypto:FindFirstChild("Buy") and Crypto:FindFirstChild("Sell") then
153         Crypto.Sell.MouseButton1Click:Connect(function()
154             local CRYPTO = Values[Crypto.Name]
155             if CRYPTO then
156                 if Balances[Crypto.Name] > 0 then
157                     Balances.Euro = Balances.Euro + Round(CRYPTO)
158                 end
159                 Balances[Crypto.Name] = Balances[Crypto.Name] - Balances[Crypto.Name]
160                 print("EURO: "..Balances.Euro.."BTC: "..Balances.Bitcoin)
161             end
162         end)
163     end
164     Crypto.Buy.MouseButton1Click:Connect(function()
165         local CRYPTO = Values[Crypto.Name]
166         if CRYPTO then
167             local Price = (Round(CRYPTO) * BUY_AMT)
168             if Balances.Euro >= Price then
169                 Balances.Euro = Balances.Euro - Price
170                 Balances[Crypto.Name] = Balances[Crypto.Name] + BUY_AMT
171             end
172         end
173     end)
174 end
175 end
176 end
177 end
178 end
```

Before testing everything out, I also made the balances functional (on the marketplace page, not on the balance page).

```
56  ▼ coroutine.wrap(function()  
57      ▼ while wait() do  
58          ▼ for _, Bal in pairs(Marketplace.Balance:GetChildren()) do  
59              ▼ if Bal:IsA("TextLabel") then  
60                  Bal.Text = Balances[Bal.Name]  
61              end  
62          end  
63      end  
64  end)
```

Now the buying and selling was functional. Finally, it was time to make crypto miners that give you a certain amount of crypto per second.



I started by designing the Interface for the miners tab. I added 4 crypto miners. The more expensive a crypto miner is the better it is.

Then, I wrote the code to buy the miners and the code to make the miners give you crypto every second. The screenshots will look darker now since I switched to dark mode.

```
91  ▼ coroutine.wrap(function()  
92      ▼ while wait(5) do  
93          ▼ if accessories["Crypto Miner 1"] == true then  
94              Balances.Bitcoin = Balances.Bitcoin + 1  
95          ▼ elseif accessories["Crypto Miner 2"] == true then  
96              Balances.Bitcoin = Balances.Bitcoin + 1  
97              Balances.Ethereum = Balances.Ethereum + 1  
98          ▼ elseif accessories["Crypto Miner 3"] == true then  
99              Balances.Bitcoin = Balances.Bitcoin + 5  
00              Balances.Ethereum = Balances.Ethereum + 5  
01              Balances.Monero = Balances.Monero + 5  
02          end  
03      end  
04  end()  
05  
06  ▼ coroutine.wrap(function()  
07      ▼ while wait(1) do  
08          ▼ if accessories["Crypto Miner 4"] == true then  
09              Balances.Bitcoin = Balances.Bitcoin + 5  
10              Balances.Ethereum = Balances.Ethereum + 5  
11              Balances.Monero = Balances.Monero + 5  
12              Balances.SLXcoin = Balances.SLXcoin + 5  
13          end  
14      end  
15  end()  
16
```

```

217  ▼ for e,v in pairs(Miners.Miners:GetChildren()) do
218  ▼    if v.Name == "m1" then
219  ▼      v.Buy.MouseButton1Click:Connect(function()
220  ▼        if Balances.Bitcoin >= 10 then
221  ▼          Balances.Bitcoin = Balances.Bitcoin - 10
222  ▼          accessories["Crypto Miner 1"] = true
223  ▼        end
224  ▼      end)
225  ▼    elseif v.Name == "m2" then
226  ▼      v.Buy.MouseButton1Click:Connect(function()
227  ▼        if Balances.Bitcoin >= 50 then
228  ▼          Balances.Bitcoin = Balances.Bitcoin - 50
229  ▼          accessories["Crypto Miner 2"] = true
230  ▼        end
231  ▼      end)
232  ▼    elseif v.Name == "m3" then
233  ▼      v.Buy.MouseButton1Click:Connect(function()
234  ▼        if Balances.Bitcoin >= 250 then
235  ▼          Balances.Bitcoin = Balances.Bitcoin - 250
236  ▼          accessories["Crypto Miner 3"] = true
237  ▼        end
238  ▼      end)
239  ▼    elseif v.Name == "m4" then
240  ▼      v.Buy.MouseButton1Click:Connect(function()
241  ▼        if Balances.Bitcoin >= 500 then
242  ▼          Balances.Bitcoin = Balances.Bitcoin - 500
243  ▼          accessories["Crypto Miner 4"] = true
244  ▼        end
245  ▼      end)
246  ▼    end
247  end

```

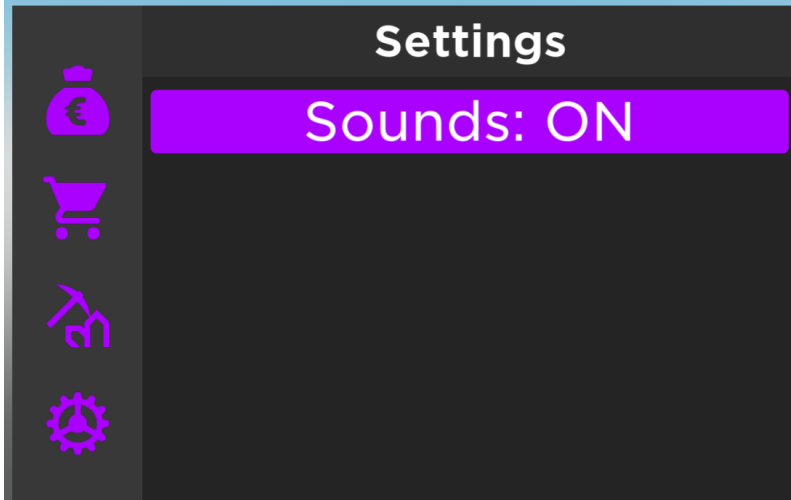
The last thing that was left to do was to make the settings tab, fix some bugs and add some small details.

```

for e,v in pairs(script.Parent:GetDescendants()) do
  if v:IsA("TextButton") then
    v.Activated:Connect(function()
      spawn(function() if Settings.Sound then script.Sound:Play() end end)
    end)
  end
end
end

```

I also added a function that plays a sound every time a player clicks a button.



In the settings tab I added a button to toggle the click sound.

Eventually, after fixing some basic bugs, the game was done. It works smoothly and I haven't encountered any problems after finishing it.

## 9. Conclusions



Overall, I enjoyed writing this TraPe and developing my game. I have learned a lot of new interesting things that I never knew before.

I find crypto currency very interesting, but I also realized the risks that come with it.

In addition, I want to study economics, finance and improve my programming in the future.

I hope you had fun reading my TraPe.

## 10. Sources

<https://www.investopedia.com/terms/c/cryptocurrency.asp#:~:text=The%20advantages%20of%20cryptocurrencies%20include,and%20use%20in%20criminal%20activities>

<https://www.forbes.com/advisor/in/investing/cryptocurrency/advantages-of-cryptocurrency/>

<https://www.analyticsinsight.net/history-of-cryptocurrencies-how-everything-started/#:~:text=The%20idea%20behind%20Cryptocurrencies,a%20truly%20decentralized%20digital%20currency>

<https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain>

<https://chain.link/education-hub/blockchain-scalability#:~:text=One%20limitation%20of%20traditional%20blockchain,participants%20to%20achieve%20high%20security>.

<https://blog.liquid.com/blockchain-scalability>

<https://www.investopedia.com/terms/p/proof-work.asp>

<https://coindcx.com/blog/crypto-basics/proof-of-work-vs-proof-of-stake/>

<https://builtin.com/blockchain/blockchain-platforms>

<https://money.usnews.com/investing/articles/the-history-of-bitcoin#:~:text=Bitcoin%20was%20the%20first%20cryptocurrency,identity%20has%20never%20been%20verified>.

[https://en.wikipedia.org/wiki/History\\_of\\_bitcoin#:~:text=On%2022%20May%202010%2C%20Laszlo,if%20held%20in%20April%202021.&text=Bitcoin%20takes%20parity%20with%20US%20dollar](https://en.wikipedia.org/wiki/History_of_bitcoin#:~:text=On%2022%20May%202010%2C%20Laszlo,if%20held%20in%20April%202021.&text=Bitcoin%20takes%20parity%20with%20US%20dollar)

<https://www.cnbc.com/2022/07/29/deloitte-75-percent-of-retailers-plan-to-accept-crypto-payments-in-2-years.html>

<https://trustmachines.co/bitcoin-history/>

<https://www.fool.com/terms/a/altcoin/#:~:text=Their%20name%20comes%20from%20the,transaction%20speeds%20or%20energy%20efficiency>

<https://crypto.com/university/what-are-meme-coins>

<https://www.investopedia.com/articles/forex/042315/beware-these-five-bitcoin-scams.asp>

<https://www.techopedia.com/cryptocurrency/is-cryptocurrency-a-good-investment#:~:text=One%20of%20the%20best%20times,buying%20stocks%20during%20a%20recession>

<https://en.wikipedia.org/wiki/Blockchain>

<https://www.cryptovantage.com/guides/safest-cryptocurrencies/>

<https://dappradar.com/rankings/chains>

