Blockchain Academy

# WORKBOOK 4


2024

## 01 BECOMING PROFICIENT WITH CRYPTO USE

According to one analyst, on average 1,500 Bitcoins are lost daily, amounting to as much as 20% of the total supply.

This is overwhelmingly due to private key or seedphrase mis-management rather than theft or hacking.


To avoid mistakes it is recommended to allocate time to practicing downloading wallets, backing up seedphrases and sending and receiving transactions prior to engaging in crypto investment strategies or transacting significant amounts of crypto.

For testing purposes use cryptocurrencies with low fees such as BSV, BCH and Monero.

Suggested practice tasks include:

- Purchasing small amounts of crypto via a decentralized exchange such as Local Monero and Paxful and immediately move purchased crypto funds to a non-custodial wallet such as Edge or Exodus.
- Make sure you have carefully backed up the seed phrase to your wallet. Once you have a test transaction appear in the wallet, uninstall the wallet then download a new wallet and import the seed phrase to reinstate the funds. Repeat this across different wallets.

Troubleshooting is one of the best ways to build knowledge and experience. Most wallets (in particular Edge) have good and responsive customer support.


- Download the website Bitaddress to your device (File / Save As). Disconnect from internet and open the downloaded webpage to create a paper or brain wallet. Send a small amount of crypto to the generated address then import the private key into a wallet application. Some wallets such as Edge and Exodus will automatically 'sweep' the address and send the crypto to a new address, incurring a transaction fee. Others such as Blockchain.com allow you to import a private key without sweeping.
- Find existing crypto addresses and investigate them on an blockchain explorer to investigate the transaction history.
- Purchase a giftcard at Bitrefill and use it to anonymously purchase an item on Amazon or other commerce site.
- Experiment with privacy techniques: choose a fiat-crypto onboarding method below to obtain some crypto then use a decentralized exchange (DEX) feature on a non-custodial wallet such as Edge or Exodus to exchange a privacy coin such as Monero and back into the original currency within the same wallet to ensure your ownership is private.

## 02 WAYS TO PURCHASE CRYPTO

The most common method to obtain crypto is via fiat purchase.



Crypto can be purchased easily and relatively safely via centralized exchanges such as Coinbase or Etoro. Fees for crypto purchases are notably low at around 1%. Crypto funds should be immediately transferred to a non-custodial wallet to avoid any potential FTX/Mount Gox event.



However, centralized exchanges require KYC (know your customer) information. Not only does this jeopardise privacy, in many countries, notably the US, crypto purchases are reported to the government tax department.

Coinbase clients have been known to receive letters from the IRS reminding them to include their crypto profits in their tax return. Purchasing crypto is itself not a taxable event, nor is holding crypto in a wallet.

However off-boarding to fiat or exchanging for a different crypto currency is considered a taxable event.

This does not always create a tax liability:

If your crypto assets devalue, this could be considered a tax deductible event.




Always check the weather forecast.

The original method to obtain crypto anonymously is to mine directly, either by choosing a coin that is ASIC-resistant (doesn't require expensive, specialized hardware to mine) such as Monero and ZCash, or by investing in an home ASIC mining rig and participating in a mining pool.

However, all mining involves financial outlay and risk due to fluctuating market price of the coin.

Other methods for acquiring crypto privately include using peer-to-peer exchanges such as Paxful, HodlHodl and Bisq. Fees are between 10-20%, depending on the method of payment. Note that payments made by bank transfers have the potential to expose your identity.


Another method is to sell fiat-purchased giftcards for crypto on sites such as Purse.io. This method works but is laborious and incurs fees.

Crypto ATMs are an option and be located via a crypto ATM map. However fees are high and increasingly the user is required to provide KYC.

One of the best way to avoid exchange fees is to accept payment for goods and services in crypto.

This can be done directly with clients or via a crypto payment gateway on a website. Both methods require ensuring clients are familiar with using crypto.

To onboard new clients to crypto, options include selling items via NFTs on platforms such as Rarible or Opensea which enable clients to purchase crypto at the checkout via creditcard.

Alternatively, clients can buy crypto directly with credit cards within wallets such as Edge and Exodus. This will require them downloading the wallet to make the purchase.


Another option to obtain crypto is to build a personal trusted relationship with an in-person trader, such as personal contacts or at crypto events. However always be aware of the risks.

## 03 PURCHASING GOODS ONLINE WITH CRYPTO

More and more websites are directly accepting payments in crypto. In addition Shopinbit, Overstock, Shopify, Bitplaza and CryptoEmporium are marketplaces listing items for sale via crpto.

Dash Direct is an app that lets you purchase goods with crypto at over 150,000 locations. Sites such as Bitrefill and Gyft purchases from a wide range of sites including Amazon, Airbnb and Uber via gift gards. Always test small value giftcards to ensure the facility is working on a given website first.

There are a wide range of crypto credit cards available on the market. These work like regular credit cards, but debit your crypto funds directly. However, expect to provide KYC unless you are able to find a prepay crypto card that works for you.


Another option is to visit places where crypto is the official currency such as El Salvador or Bitcoin Island in the Philippines. You can also use the website BTCMap to find locations internationally that accept Bitcoin.

REMEMBER, you too can be a driver of adoption by encouraging stores and retailers to accept crypto. Get inspiration on how to live entirely from crypto here.

## 04 BEYOND BITCOIN: OTHER CRYPTOS & BLOCKCHAINS

Numerous cryptocurrencies have evolved into the space since Bitcoin. While it is not possible to know all (currently over 9,000 listed on Coinmarketcap), it is important to understand the most important categories. Here is a list of the main types:

**Smart Contract Blockchains**

Ethereum was the first blockchain to fully focus on integrating Turing completeness into its protocol by innovating smart contract technology within a decentralized node network. This led to the development of the ERC20 smart contract standard, enabling alternative coins (alt coins) to become easily and rapidly deployed on top of the Ethereum blockchain.

Smart contract technology has led to decentralized finance (DeFi) protocols and, more recently, NFTs. Examples of other smart contract platforms include Cardano, Solana, Polkadot, Binance, Avalanche, Tron and BSV.

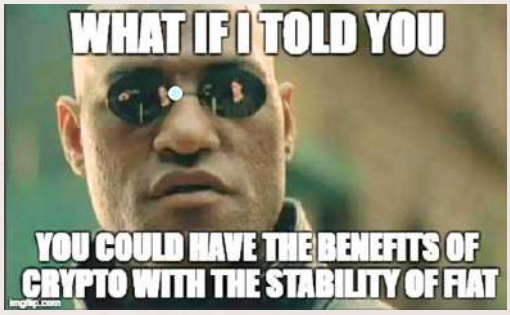
**DeFi coins**

A DeFi coin is a cryptocurrency specifically associated with the decentralized finance ecosystem and used within DeFi protocols to serve various functions such as governance, incentivization, staking, liquidity provision, or as a means of exchange within the DeFi ecosystem. The majority of DeFi innovation takes place on top of Ethereum although DeFi is also being innovated on other smart contract platforms.

Leading protocols (coins) include Chainlink, Uniswap, Aave, Maker and Compound. The main function they serve is to provide lending and borrowing liquidity pools, although the utility of each coin often have additional functions such as governance participation, incentivization, payment, or liquidity provision within the ecosystem

## Stable Coins

Stablecoins are a type of crypto currency designed to maintain a stable value relative to an asset, typically a fiat currency like the US dollar, aiming to providing stability and hedge against the volatility of other cryptos. Examples of stable coins include Tether, USD Coin, Dai and Binance USD.




## Quantum Resistant Blockchains

A quantum-resistant blockchain is a blockchain that incorporates cryptographic algorithms and techniques that are resistant to attacks from quantum computers. According to theory, a quantum computer might have the computational power to brute force the cryptographic algorithms currently used to secure data and transactions on traditional blockchains.

Quantum-resistant blockchains are designed to protect against this threat by implementing quantum-resistant cryptographic algorithms. Examples include QRL, IOTA and QAN Platform.

No blockchain algorithm has been broken by quantum computers at this time and the current state of the technology is still limited by the number of qubits, coherence time and error rates.

## Asic Resistant Blockchains

ASIC resistant blockchains are designed to resist the dominance of specialized mining hardware devices known as ASICs. ASICs are custom-built machines specifically optimized for a particular algorithm, in particular the SHA-256 algorithm used in Bitcoin mining. They provide significantly higher computational power and energy efficiency compared to general-purpose computer hardware like CPUs or GPUs.

The main objective of ASIC resistant blockchains is to promote a more decentralized and egalitarian mining environment by ensuring that mining can be performed with commonly available hardware, such as CPUs or GPUs. Examples include Ethereum which uses Ethash mining algorithm and Monero which uses Random X algorithm.

## Governance Tokens

Governance tokens are a type of cryptocurrency or digital token that grants holders the right to participate in the decision-making and governance processes of a blockchain platform or decentralized organization. Governance coins are often associated with decentralized autonomous organizations (DAOs), decentralized finance (DeFi) platforms, or other blockchain projects that emphasize community-driven decision-making.

Examples of governance coins include Maker (MKR) in the MakerDAO ecosystem, Compound (COMP) in the Compound protocol, and Uniswap (UNI) in the Uniswap decentralized exchange.

**Privacy Coins**

Privacy coins are cryptocurrencies that prioritize and enhance the privacy and anonymity of transactions and user information on the blockchain, employing various cryptographic techniques and protocols to obfuscate transaction details, sender and recipient identities, and other sensitive information associated with transactions.

Examples include Monero, Zcash, Dash and Dero, the only smart-contract, privacy-focused blockchain.

**Microtransaction Coins**

Microtransaction coins are cryptocurrencies designed to facilitate small-value transactions or microtransactions. These coins enable quick, low-cost, and efficient transfer of tiny amounts of value, typically below the threshold of traditional payment systems.

The main goal of micropayment coins is to enable seamless and cost-effective transactions for digital content, online services, and other small-scale transactions that would otherwise be impractical or expensive to process using traditional payment methods in various scenarios, such as content monetization, online gaming, pay-per-view services, and more.

Examples include BSV, Nano, IONTA. Bitcoin Cash and Polygon can also be thought of as microtransaction coins, although the fees are around 1 cent.

## Interoperability Blockchains

Interoperability blockchains aim to connect multiple independent blockchains, allowing for the transfer of assets and data across different networks.

They facilitate cross-chain communication and interoperability, enabling compatibility and cooperation between disparate blockchain platforms. Examples include Polkadot (DOT) and Cosmos (ATOM).

## Meme Coins

Meme coins, also known as joke coins or meme-based cryptocurrencies, are a category of cryptocurrencies that have gained popularity primarily for their humorous or satirical nature rather than their underlying technology or utility.

These coins often derive their value from internet memes, viral trends, or cultural references. Meme coins have captured significant attention in the cryptocurrency space, particularly during the recent surge of interest in cryptocurrencies and decentralized finance.

Examples of popular meme coins include Dogecoin (DOGE), which originated as a joke based on the Shiba Inu dog meme, and Shiba Inu (SHIB), which gained popularity due to its association with Dogecoin and the larger meme coin culture.

# 04 INVESTMENT STRATEGIES

Often people are attracted to crypto due to widespread stories of huge profits being derived from crypto investing. However investing in cryptocurrencies is no different to investing in any other asset class or industry; profit is derived from risk and successful investing relies on the ability of the investor to correctly analyse that risk and implement effective risk management strategies such as in-depth market research and portfolio diversification.

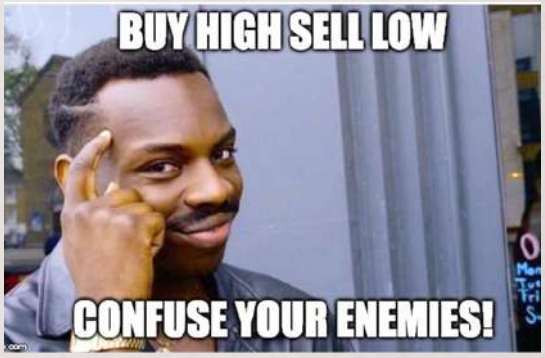
There are equal stories of money being lost either from poor investment decisions, often based on emotion rather than strategy.  When considering investing into the cryptocurrency space it is important to conduct extensive personal research and adopt a wise investment approach that protects you against risk.

From a libertarian perspective the best investment is considered to be in the adoption of the technology itself and the liberation and sovereignty decentralized finance offers society.

That being said, financial investment in crypto can be positive and result in increased financial and personal freedom.

We will compare some key investment methods.

But first we dedicate a page in this workhops to crypto investment memes. We hope you enjoy.

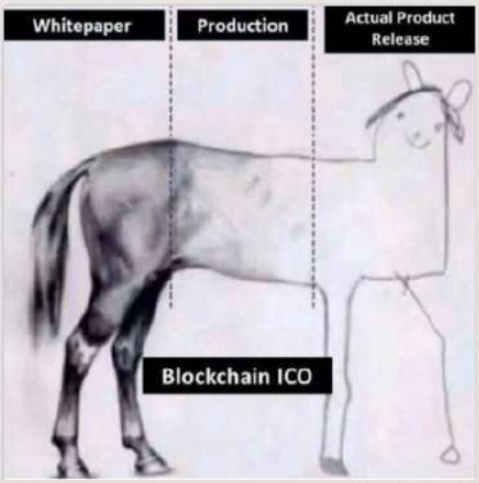


## VOLITION LABS CRYPTO INVESTING MEME UNIVERSITY











Crypto investing rule #1: Don't be these guys.

## HODLing

HODLling refers to the strategy of purchasing crypto for the longterm, regardless of short-term market fluctuations. The origin of HODLing originates from a now infamous Bitcoin Forum incident.


The rationale behind the HODLing investment approach is based on the view that deflationary cryptocurrencies, notably BTC, will appreciate over time in contrast to inflationary fiat currencies such as the dollar.

HODLers believe that over time this strategy will outperform crypto market fluctuations.


The HODLers were right: despite market fluctuations, BTC made 177,500% gains between 2012 and 2022.
Source: https://thesmallbusinessblog.net/crypto-statistics/


When holding crypto for the long term, investors should consider cold storage of funds and inheritance provisions.

## ICOs

Initial Coin Offerings are fundraising methods used by cryptocurrency and blockchain projects to raise capital by issuing and selling tokens to investors.

ICOs gained popularity during the 2017 crypto boom after Ethereum made it possible to generate and deploy alt coins via smart contracts and have since become a prominent way for projects to secure funding for development and operations.

During an ICO, a project issues its own cryptocurrency tokens, often based on existing blockchain platforms. These tokens are typically designed to serve a specific purpose within the project's ecosystem, such as accessing services, participating in governance, or representing a stake in the project

ICOs often have different sale phases, including private sales, presales, and public sales. Private sales are usually available to early investors, while presales offer tokens to a larger pool of investors at a discounted price. The public sale, also known as the main ICO, is open to the general public.



ICO investments carry risks, including the potential for scams, lack of regulatory oversight, project failures, and price volatility. Due diligence is essential before investing in an ICO, including reviewing the project's whitepaper, team background, technology, community engagement.

## Trading

There are many people making full-time income from cryptocurrency trading. However this is a high-risk activity, requiring concentration and dedication. In general it is professional, full-time traders who make continual gains.

When starting to trading cryptocurrencies, it is advisable to experiment with paper trading for at least a year before progressing to live trading. This provides the opportunity to study and test a number of trading strategies.


An alternative strategy is to copy trade successful traders via apps such as Etoro.

Types of trading include day trading, swing trading, position trading, scalping, momentum trading and breakout trading

## DeFi

Decentralized Finance refers to a financial system built on blockchain technology that aims to provide open, permissionless, and inclusive financial services as an alternative to the central banking system.

Unlike traditional finance, which relies on centralized intermediaries such as banks, DeFi operates on decentralized networks, primarily utilizing smart contracts on blockchain platforms like Ethereum.

DeFi protocols provide access to a number of facilities previously only available within centralized banking. These include staking crypto into liquidity pools to accumulate interest, leveraging additional finance through loans and creating and trading synthetic assets that represent real-world assets such as stocks, commodities or fiat.

Currently all leading (by market cap) DeFi platforms run on Ethereum including Maker DAO, Aave, Compound, Uniswap and Synthetix.


DeFI can be accessed through wallets such as Edge, Trust, DeFi Swap, Ledger and Trezor.

Edge wallet features one-click staking of coins, providing a simple way to try staking as an investment strategy.

**NFTs**

Non-Fungible Tokens, are unique digital assets that are represented and authenticated on a blockchain, using smart contract blockchains such as Ethereum, Tezos or Solana.

Unlike cryptocurrencies such as Bitcoin or Ethereum, which are fungible and can be exchanged on a one-to-one basis, NFTs are indivisible and represent ownership or proof of authenticity of a specific item or piece of content.

NFTs are fast disrupting the traditional art world, due to their ability to prove the provenance of an artwork as well as deliver recursive sales dividends to the original creator via smart contracts.

For many people NFTs represent a more practical way to invest in art since they can be stored simply in a smart device.

NFTs can be created and purchased by connecting a wallet such as Metamask to NFT platforms such as Opensea or Rarible which create and deploy simple NFT smart contracts via easy-to-use interfaces.


**Infrastructure and support industries**
Another option is to invest in companies that are building out real-world blockchain use cases such as user-led content platforms, supply chain tracking and communications and data management protocols.

Equally there are investment opportunities within a wide range of support industries including education, information and software development.