

# THE PAST, PRESENT & FUTURE OF MONEY

---

A comprehensive analysis of money throughout time and how cryptocurrency is the next, and potentially most disruptive chapter



**Platypus**  
TERMINAL

PART:

1

○  
THE  
PAST

|  
What is Money?  
Paper Money

2

○  
THE  
PRESENT

|  
Macroeconomic Environment  
Financial Crisis  
Inflation

3

○  
THE  
FUTURE

|  
International Monetary System  
What is the Blockchain?  
Proof of Work/Stake/Authority  
Smart Contracts  
Decentralized Finance – DeFi  
Public Backing  
Supply  
Cryptocurrencies Greatest Flaws  
Tokenisation

4

○  
THE  
TOP SIX

|  
Bitcoin  
Ethereum  
Tether  
Binance Coin  
Cardano (Ada)  
Dogecoin



# WHAT IS MONEY?

Since the dawn of time, humans have been exchanging goods and services to fulfil needs of survival and pleasure. The first and most integral question that must be answered when exploring the Past, Present and Future of Money is; what is Money in its simplest form?

Money is often described using a number of fundamental characteristics that underpins its utility to users. Before the creation of modern 'paper money,' commodity money was first used to identify and transact value, as determined by geography and the nature of individual economies.

For example, shells, copper, gold, silver, sugar and rum were all used as forms of commodity money. Together they maintained five rough characteristics: Used for thousands of years, commodity money

## PART ONE: THE PAST



SCARCITY



RECOGNIZABILITY



DIVISIBILITY



PORTABILITY



EXCHANGEABILITY

allowed individuals, businesses and ruling powers to transact in a functioning economic system. In its purest form, money overcomes the need for barter within an economy where two individuals directly exchange an agreed amount of goods.

One of the most common commodities used as money were solid metals such as gold, silver and bronze, which all satisfy the above conditions. The earliest known use of metals as commodity money can be dated back over 8,000 years ago to the Mesopotamian Shekel made from silver.<sup>1</sup>

Commodity Money is, however, subject to debasement, the process of reducing the quality or value of coins. This can be done by reducing the content of precious metal in a coin by adding base metals.

In essence, when a currency is debased, a central body is electing to lower the value of a currency which is known to cause inflation, easing the fiscal pressures of paying off government debt.

When the value of a currency, whether commodity or paper, is devalued through the increase in supply, more money competes for the same amount of goods and services, increasing prices.

However, this is done at the expense of the purchasing power of an economy's citizens, with each unit of the currency becoming proportionally less valuable. The process of manipulating the money supply is through debasement, which is thousands of years old.





# PAPER MONEY

Some of the largest inefficiencies with commodity money included its ability to be stored and transported, its perishability, and variation in quality. The earliest evidence of Paper Money to solve these issues dates to 617-907 BC during the Tang Dynasty in China, where for a fee, merchants could deposit funds at a counting house<sup>2</sup>. This secured the safety of their funds and allowed them to draft checks to third parties against those deposits at the counting-house.

During the Song Dynasty in the late 9th century, an increased supply of iron coins led to periods of heightened inflation and a loss of confidence in the currency. A revolt led to the closure of the Iron Mints, and an extension of the Tang Dynasty's paper money was issued in its replacement and backed by 16 deposit-taking institutions. They held the physical currency rather than its user carrying excessive amounts of coinage.<sup>3</sup> This then allowed individuals to transact using notes from these institutions.

It wasn't long before these institutions realized they had the ability to essentially print money by issuing more currency on paper than they had in reserve. Eventually, a market panic where individuals tried to withdraw their deposits led to bank failures and the eventual bailout of these institutions by the government. In 1022, paper money was nationalized, placing the government in control of the money supply.

The Song Dynasty financed infrastructure projects, war, and other spending by printing money, realizing the benefits of increasing the money supply. This led to a period of economic prosperity.<sup>4</sup> Over the next 100 years, the total money supply would increase twenty-fold, eventually leading to a period of hyperinflation and civil war. The Travels of Marco Polo to China and Mongolia would bring the concept of paper money back to Europe during this period.



Paper Money from the Song Dynasty (Jiaozi)

---

Ancient China exhibits the first significant transition away from commodity money to paper money. However, what must be recognised about paper money is that its value lies in trust. Individuals trusting the party or body that holds, owes, or governs the paper and its prescribed value, underpins the entire system.

---

Collectively, Australians value a \$50 note because they trust that banks, the government and others in society collectively recognize the value in the paper-thin piece of plastic.

Paper money maintains the characteristics given by commodity money. Modern economics as well as the Reserve Bank of Australia, prescribe the following three attributes to all modern forms of money.<sup>3</sup>

The Attributes of  
Money



A Unit of  
Account



A Store of  
Value



A Medium of  
Exchange



# MACROECONOMIC ENVIRONMENT

Our current macroeconomic environment is dominated by the role of Governments and Central Banks dictating the direction of Fiscal and Monetary Policy.

The Netherlands established the first modern central bank in 1609, with the aim of both achieving economic stability but also to strengthen the future prospect of the domestic economy.

In the centuries to come, the Dutch became an imperial powerhouse in Europe alongside the English, French, Spanish and Portuguese, who all eventually established central banks.

PART TWO:

THE PRESENT

CENTRAL BANKS ARE TRADITIONALLY TASKED WITH A VARIETY OF MANDATES THAT INCLUDE:



FINANCIAL STABILITY



PRICE STABILITY



ECONOMIC GROWTH

Achieving these goals is done through the combination of policy tools, including setting a central interest rate and quantitative easing. These tools together contribute to the control of money and credit within an economic system.

For example, the cash rate is used to increase and decrease the supply of a currency. A reduction in the cash rate means financial institutions can borrow and lend more freely in the overnight money market, going on to lower other interest rates throughout the economy. Lower interest rates means banks, businesses, and individuals can borrow money cheaper, incentivizing them to do so and hence, increasing economic activity.

In addition to Interest Rates, central banks in recent decades have also utilized Quantitative Easing (QE), which essentially reflects an ability to print money. QE involves central banks creating money out of thin air to buy assets from financial institutions, most often Government and Corporate Bonds. These bonds sit on the central bank's balance sheet and inject liquidity into the financial system.

This demand for bonds increases their price, forcing yields lower and leaving investors searching for higher-yielding assets. The demand for supplementary assets drives their prices higher and yields lower, causing a flow-on effect throughout the economy. This creates the desired effect of pushing interest rates within the economy lower and stimulating economic activity once again. A major criticism of QE, however, is that it drives asset prices higher, increasing the wealth of those who own those assets.

The ability for central banks to essentially create money from nothing can be very powerful during times of crisis. At the onset of the COVID-19 crisis, central banks worldwide cut interest rates and implemented Quantitative Easing programs, to support economies and inject liquidity into the financial system. This power, however, comes with great suspicion and responsibility.



# THE FEDERAL RESERVE

The Federal Reserve was established in 1907 after 100 years of volatile economic conditions in the US to achieve economic stability. The Panic of 1907 led to a run on the banking system, the default of major Banks and eventually the establishment of the Federal Reserve.

Rather than being established in Washington, negotiations were held on Jekyll Island in Georgia on a private property with 100 of America's most powerful men.

After 5 years of negotiations, the Federal Reserve was established, though was structured like no central bank before it.

A network of 12 regional banks were established, each with their own governor reporting to the Federal Reserve Board independent of the US Government. The most unique aspect of the Federal Reserve lies in its ownership.

Banks in the US must keep 6% of their capital in regional reserve banks as deposits awarding them proportionally with shares in that regional Reserve Bank. These shares cannot be sold or traded and are pegged at \$100 per share. They only provide voting rights for two-thirds of the Regional Reserve Board.

Essentially, the major Banks all own the Federal Reserve, though many conspiracies have shrouded this ownership, with control by the famous Rothschild Family touted as the most suspicious.<sup>1</sup>

# FINANCIAL CRISIS

Though our current economic system functions with exceptionally high efficiency, it is like any, subject to periods of turbulence over time. In recent decades, central banks have been accused of contributing to heightening inflation in many economies.

Governments have taken on excessive debt levels to support their domestic economies, and the risk taking by financial institutions has wreaked havoc on asset markers. The powers given to these institutions have often been abused and mismanaged, leading to financial crisis and putting into question their ability to efficiently run economies.

# INFLATION

According to the Reserve Bank of Australia (RBA), "Inflation is an increase in the level of prices of the goods and services that households buy."<sup>2</sup> Inflation is also a part of a central banks mandate, with the RBA's target inflation being 2-3% per year.

Inflation is a healthy by-product of a growing economy as it displays the growing wealth and activity of its components. Inflation has closely been associated with an increase in the money supply over time.

However, as mentioned previously, inflation erodes the purchasing power of currencies over time. Government and central mismanagement of the money supply over the last 100 years has led to hyperinflation in countries such as Germany, Hungary, Zimbabwe, Greece and Venezuela.

THOMAS JEFFERSON



"I Believe that Banking Institutions are more dangerous to our liberties than standing armies!"

MILTON FRIEDMAN



"Inflation is always and everywhere a monetary phenomenon in the sense that it is and can be produced only by a more rapid increase in the quantity of money than in output."



# INTERNATIONAL MONETARY SYSTEM

The future of the international monetary system as it is known today is currently in the midst of a seismic shift in how Individuals, Corporations, and Institutions transact. Cryptocurrencies attempt to provide the answer to a financial system that is not owned, controlled, backed or profited from by central authorities who maintain power over the system.

In the previous section, “the present,” the power of governments, central banks and financial institutions directly determines the supply, demand, and direction of money. This power is easily corruptible, which has been proven over history, often leading to the financial crisis and unequal wealth distribution. The most well-known cryptocurrency, Bitcoin and many others were created with the direct intention of taking away the power of these bodies and placing it in the hands of the people who collectively assign a currency value. The Whitepaper for Bitcoin written by Satoshi Nakamoto, opens by addressing E-commerce’s reliance on “financial institutions serving as trusted third parties to process electronic payments”<sup>1</sup>, and how this model suffers from inherent weaknesses.

The majority of the developing world is subject to a lack of access to finance and backing, weighed down by weak economies, corrupt governments and unstable currencies. The concept of an international currency backed not by banks or governments, but by the individuals that use it could provide billions of people access to a world of finance and commerce that was previously inaccessible.

---

For example, the developing world’s access to credit is severely limited because major institutions find little profitability from investment in these regions. An international currency is posed to provide spending, lending and investing to all corners of the world, not based on location, geography, or wealth.

---

The proposal of carrying out third-party intermediaries will also significantly reduce the transaction costs when using a cryptocurrency. Financial intermediaries are designed to create transactions cost for a service provided between two parties. A currency controlled and owned by the people that does not rely on an intermediary would see lower transaction costs and increased efficiency.

As mentioned previously, the most integral part of something having value is the trust and backing of those who use it. If society collectively trusts that a cryptocurrency has value and allows supply and demand in an open market to determine its price, then it is just as valuable as a Euro or Dollar.

The theory behind cryptocurrency’s transforming the world economy may sound encouraging and contain a range of benefits; however, what really are they, and how does the technology behind them work?

PART THREE:

THE FUTURE





# WHAT IS THE BLOCKCHAIN?

Blockchain Technology can be defined as "a distributed database of records or a public ledger of all transactions or digital events that have been executed and shared among participating parties."<sup>2</sup> Essentially, blockchain is a database of information. As the name suggests, a blockchain incorporates data stored in blocks that are chained together. Each block in this chain contains the following:

## Data

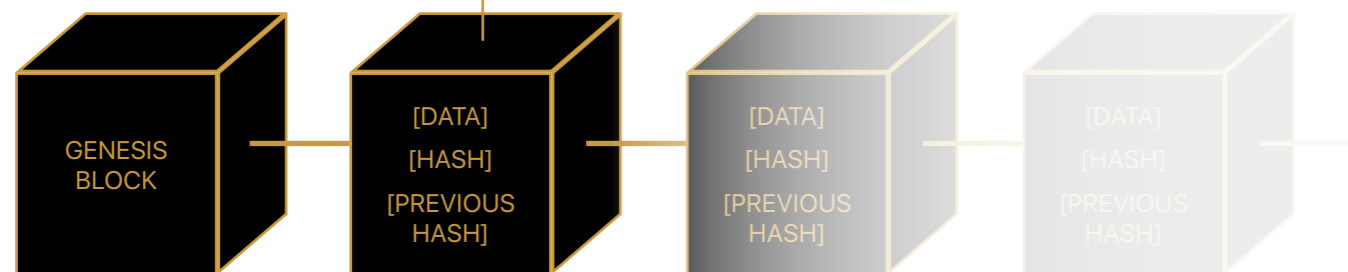
For a transaction of a cryptocurrency, this would involve the sender's address, receiver's address and transaction amount.

## A Hash

A Hash is a unique identification number for each individual block.

## Previous Hash

The chain is created by linking each block to the previous one using a Hash.



## Genesis Block

The first block in this chain is known as the genesis block as there is no Hash from the previous block to use. Starting with the genesis block, the following blocks that are linked together essentially act as a public ledger of all transactions that have ever taken place.

## Peer to Peer Network

The term 'peer to peer network' is used to describe how this ledger is public, and once a user joins the blockchain network, they get a copy of the blockchain itself. This means all members/computers/nodes will have access to the users' address and transaction details; however, the identity behind the user's address is completely anonymous.

## But how are new blocks added?

Before a block is added to the blockchain, it must be first verified by the users/nodes of the network. Once verified, the block is created, added to the blockchain, and then viewable to all network users. The interconnection of the entire network holding the ledger and verifying each transaction makes it extremely secure and less prone to cyber-attacks.

Some users within the blockchain network are known as miners, responsible for adding new blocks onto the blockchain by verifying transactions. The methods of Block verification are Proof of Work, Proof of Stake, and Proof of Authority.

Image: Cryptocurrency Mining, Reykjavik Iceland



# PROOF OF WORK / STAKE / AUTHORITY

## PROOF OF WORK

Proof of Work begins with a transaction being submitted to the network. Nodes/Users then compete to solve a complex mathematical problem to find a key known as the nonce. This nonce is validated by the rest of the network as the true answer to the mathematical problem, allocated a Hash key, and added to the blockchain.

The Bitcoin Whitepaper described this process as the "scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits."<sup>2</sup> The node is then given a reward for completing this process, often coins. In Proof of Work, the larger the computational power of the node, the more transactions and blocks they are able to verify and add to the blockchain.

This means that nodes with more computing power are able to verify more transactions, making the cost of physical equipment and the cost of electricity, key components in the profitability of mining.

Countries with low electricity costs, such as China and Eastern Europe hence experience greater blockchain mining activity. The reliance on raw electricity has, however, led to a wide number of environmental concerns surrounding the proof of work structure. Recently, provinces in China, the world's largest Bitcoin miner, have cracked down on cryptocurrency mining, completely outlawing mining farms. These farms require enormous amounts of power and have been known to cause power outages on the surrounding grid.

## PROOF OF STAKE

An alternate to Proof of Work is Proof of Stake, which gives mining power proportionate to the number of coins (a stake) held by that miner. For example, if you own 10% of the total supply, you will have the ability to process 10% of the transactions. This means that your ability to mine and approve transactions is proportional to how many coins you have, not computational power.

In the Proof of Stake system, there are no miners but instead validators and forgers who are contributing to the network for a constant reward.<sup>3</sup> The Rewards given are specific to the type of cryptocurrency and are dependent on a variety of factors.

Proof of Stake can hence act as a form of passive income, a process known as staking. Different cryptocurrency projects may have barriers to do so, but investors can stake in a variety of ways:

- **Individually:** Using your own wallet and computer.
- **On an Exchange:** using an intermediary is usually the easiest and most accessible, though you must pay a fee and have no control over your coins.
- **In a Staking Pool:** Groups of people staking together is similar to an exchange, still requiring a fee though it may not be transparent and forces you to give up your private key.
- **Validator as a Service:** Company sets up a wallet computer, and you are in control of your coins but still pay a fee.

## PROOF OF AUTHORITY

Finally, proof of authority is the most centralized of all, with pre-approved actors given permission to validate transactions.

Proof of Authority essentially gives selected individuals' monopoly power on the system, allowing them to validate only the transactions they desire. Hence, this makes corruption possible and is subject to system failure if those with authority are compromised.

## ALTERNATIVE USES

Blockchains are also not cryptocurrency specific, all operating on their own unique and decentralized networks. Blockchains can be used to store information for:

- **Monitoring Supply Chains:** Removing paper trails and allowing customers and businesses to track goods and services better.
- **Digital Voting:** Regulators would clearly be able to see if the network was manipulated.
- **Tax Regulation and Compliance.**
- **Data Backup, Storage and Sharing.**
- **Medical Record Keeping:** Moving away from computer and cloud storage.
- **Weapons Tracking:** Weapons accountability.



# SMART CONTRACTS

The term 'Smart Contract' was first coined in 1997 by computer scientist and cryptographer, Nick Szabo. With the same functionality as a real-world contract, a smart contract is a computer program stored within a block in the blockchain. It has sets of terms and conditions that must be fulfilled by both parties and lays contingencies for them.

Each Smart Contract has two key characteristics:



## It is Immutable

Meaning once created, it cannot be modified.



## It is Distributed

Meaning that the output of the contract is validated by the network it operates on.

Nick Szabo used the following analogy to describe Smart Payments in his publication, "Formalizing and Securing Relationships on Public Networks"<sup>14</sup>:

*"A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. A vending machine is a contract with a bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas."<sup>14</sup>*

Some real-world applications of Smart Contracts on the Blockchain include; loan payments, processing insurance claims, or paying for postal on delivery. In some sense, the enforcer or third party in these transactions are the code and guidelines of the

smart contract itself, and a network of nodes verifies its enforcement. This use of technology to enforce contracts signed between two or more parties leads us to a world of finance without centralized institutions.

# DECENTRALIZED FINANCE – DEFI

Today, the financial markets are centralized, from the Stock Market, Banking to Insurance. These central bodies are prone to mismanagement, fraud and corruption, and profit from being third parties in the current system. Cryptocurrencies and Blockchain Technology provide an opportunity to grow a decentralized, or DeFi, Financial system where the financial services do not require a central authority.

This is arguably the end game for cryptocurrency to replace or at least provide an alternative to our current financial system. Naturally, this proposition has been met with opposition. For example, the American Bankers Association stated in June 2021 that, "The United States should not implement a central bank digital currency, simply because we can or because others are doing so," and that the benefits are "theoretical" and the consequences "severe."<sup>5</sup>

The blockchain is the infrastructure behind this decentralized system. This system must then operate on a programmable platform where services can be provided to users. One of the most popular and commonly used is the Ethereum network which, unlike Bitcoin, can have applications integrated and adaptations made. Here are two examples of Decentralized Services.

- A Decentralized Exchange or DEX resides on the Ethereum platform and operates without a central authority. This exchange allows the purchase and sale of cryptocurrencies with no account, ID verification or fees.

Despite its transparency, this system also poses inherent risks, such as the exploitation of loopholes by hackers and the faulty construction of smart contracts. Some products or services also maintain a level of centralization, which can be exposed as a major flaw in their core purpose. Like all industries, fraud and corruption remain a risk.

- Next, a Decentralized Money Market connects borrowers and lenders, providing arguably one of the essential financial services. This decentralized money market would allow you to deposit cryptocurrency as collateral and borrow against it at a predetermined interest rate. For example, Compound is an Ethereum protocol that automatically connects borrowers and lenders to provide the functions of a money market.<sup>6</sup> Through smart contracts, the terms of loans are enforced by the platform and the interest distributed accordingly. One of the most popular functions of this money market is utilizing the blockchain to allow people to earn interest on cryptocurrency they loan out on the blockchain. This process is known as yield farming and has become more popular on the network.

For individuals to use these services, a less volatile currency is needed. Hence, Stable coins were created to provide users confidence in the system. Stable coins are pegged to a real-world asset such as the US Dollar, providing users confidence in the system and products they use. DeFi clearly provides the infrastructure for a revolutionized financial system free from central authority and transaction costs.





# PUBLIC BACKING

As mentioned previously, the importance of collective trust in a cryptocurrency forward world economy requires backing by public figures, governments, and institutions.

Together, they provide demand and liquidity to cryptocurrency markets but, most importantly, provide confidence to the general population that others trust the currency.

- Famous Investors such as Paul Tudor Jones, Jack Dorsey, Stanley Druckenmiller, Mark Cuban
- Companies such as PayPal, Starbucks and Wholefoods
- Central Banks around the world have also explored the creation of their own cryptocurrency.
- El Salvador became the first government to mandate Bitcoin as legal tender in June 2021
- Celebrities such as Jay-Z, Mike Tyson, Snoop Dog

Arguably, the notable of all is Elon Musk, who, throughout 2021, contributed significantly to volatility within cryptocurrency markets. The Billionaire Entrepreneur issued a variety of comments on Twitter, addressing Bitcoin, Dogecoin, and Ethereum, which had positive and negative impacts on cryptocurrency markets.

Elon Musk @elonmusk  
ur welcome



221K Retweets 12.3K Quote Tweets 823K Likes

Elon Musk @elonmusk  
Bitcoin is almost as bs as fiat money

7.4K Retweets 2.2K Quote Tweets 94K Likes

Elon Musk @elonmusk  
Bitcoin is my safe word

2.5K Retweets 5.6K Quote Tweets 36K Likes

Elon Musk @elonmusk  
To be clear, I strongly believe in crypto, but it can't drive a massive increase in fossil fuel use, especially coal - It is high time there was a carbon tax!

16K Retweets 6.3K Quote Tweets 39K Likes

Elon Musk @elonmusk  
You can now buy a Tesla with Bitcoin

10K Retweets 37K Quote Tweets 151K Likes

Elon Musk @elonmusk  
Tesla is using only internal & open source software & operates Bitcoin nodes directly. Bitcoin paid to Tesla will be retained as Bitcoin, not converted to fiat currency

1.3K Retweets 7.4K Quote Tweets 41K Likes

Elon Musk @elonmusk  
No highs, no lows, only doge

118K Retweets 11.2K Quote Tweets 781K Likes

# SUPPLY

Today, central banks have complete control over the supply and demand of money, a group independent of the public and government.

They can print money at will, increasing the money supply and devaluing a currency. The concept of a decentralized token currency takes away a central bank's power to manipulate the supply and demand of a currency.

Most cryptocurrencies have no central body governing the supply of the currency itself, leaving it either fixed or at a determined growth rate. For example, the largest cryptocurrency by market capitalization, Bitcoin, has a fixed supply of 21,000,000 million coins.

A distinction must be made when referring to coins with an unlimited supply. While technically true, these currencies actually grow at a predetermined interest rate each year. For example, Dogecoin has a fixed growth rate of approximately 5.5 billion coins per year, currently representing an inflation rate of 5 percent. The comparison can then be made against traditional currencies, which can be manipulated at will, having a variety of consequences upon economies.



# CRYPTOCURRENCIES' GREATEST FLAWS

The most significant threat to the long-term success of cryptocurrency is regulation by government bodies. The concept behind a decentralized financial system circumvents the centralized system currently in place. This, in turn, takes away the powers given to those in authority, at central banks, governments and the financial industry.

It is in the government's inherent purpose to regulate markets to ensure fair competition. As cryptocurrencies expand in use and relevance as they have done over the last decade, the more attention they will receive from governments and those in power and in turn leading to further regulation.

Cryptocurrencies, due to their anonymity, are often used for criminal purposes. Due to their untraceable nature and disconnection from any government institutions, they can be used for tax evasion and money laundering. In particular, Bitcoin's early implementation into the dark web propelled its status worldwide.

---

This association with crime places even more onus on governments to regulate cryptocurrency markets and limit their implantation into our current financial system. In truth, a report conducted by Chainalysis' criminal activity represented just 2.1 percent of all transactions in 2019<sup>7</sup>.

---

The words of individuals such as Charlie Munger (see right), Janet Yellen, and other prominent figures within the world of finance have pushed this narrative.

CHARLIE MUNGER



"Of course, I hate the Bitcoin success and I don't welcome a currency that's useful to kidnapers and extortionists, and so forth"

RAY DALIO



"Bitcoin's greatest risk is its success"

# TOKENISATION

## NON-FUNGIBLE TOKENS (NFT)

Bitcoin can be described as fungible, as one bitcoin is exactly the same as another and has the same characteristics. Something Non-fungible is completely unique and can come from a video, piece of art or even music.

Non-Fungible tokens are uniquely created, digitally registered and lodged on a blockchain, with most NFT's currently existing on the Ethereum blockchain.

The most expensive purchase of a unique NFT was an artwork called Everyday – The First 5000 days (shown behind), which is a compilation of many artworks in one image. At Auction, this piece of art was bought for US\$69 million.

## REAL ESTATE TOKENIZATION

Blockchain Technology has the ability to tokenize property much like it has cryptocurrencies and other assets, allowing them to be traded in the same way. Real Estate Tokenization refers to dividing property into tradeable, divisible and digital assets on a blockchain.

Though it is extremely difficult to do this directly, specific vehicles can be used to act as the token that transacted on the blockchain. For example, an investment company who directly owns a set property or list of properties can have its ownership tokenized and yield from the property paid out to the token holders.

The tokenization of property will remove the most prominent barriers to entry in the industry such as upfront capital costs and overhead costs. Tradeable Real Estate tokens also give property a divisible characteristic, allowing it to be traded 24/7, giving live and more accurate pricing. This means that investors of any size will be able to own property with more visibility, transparency, and liquidity.



## PART FOUR: THE TOP SIX



# #1 BITCOIN

Inception: January 2009 | Supply: 18.74M | Max Supply: 21M



The largest cryptocurrency by market capitalization and often synonymous with the asset class is Bitcoin. Bitcoin was created in 2008 by Satoshi Nakamoto and is generally accepted as the first cryptocurrency to be created. The enormous success of Bitcoin can be tied to a combination of factors, though most importantly, its first-mover advantage. Bitcoin promoted both the potential of cryptocurrency but also blockchain technology itself, breaking into the mainstream in a short period of time.

Bitcoin uses a proof of work verification system to verify blocks on its own blockchain. Mining on the Bitcoin Blockchain is subject to a process called halving, which is the method by which new coins are distributed to nodes. The halving process occurs after approximately every 210,000 new blocks are added to the blockchain by miners and is enforced by the Bitcoin Code. This ensures a steady and predictable rate of new coins being distributed onto the system. Initially, the protocol rewarded miners with 50 Bitcoins every 10 minutes; however, currently, it is just 6.25. It is expected for the entire 21 million maximum supply of Bitcoin to take approximately 120 years to mine because of the halving process. A major threat to the acceptance of Bitcoin as a legitimate mode of transaction is tied to the environmental concerns mentioned previously. Bitcoins use of a proof of work system means that computational power must be expended to verify blocks on the blockchain. Over time, the physical power required to mine each coin increases, meaning stronger computers and more electricity. The intense amount of computational power to mine bitcoin means it takes 10 minutes to mine just one coin.

### SATOSHI NAKAMOTO

Satoshi Nakamoto is the pseudonym used for the individual who created bitcoin. The true identity of this individual remains a matter of dispute with investigations and conspiracy theories pointing to the individual being a group of European Banks, Elon Musk, and Computer Programmers worldwide. Satoshi also has an estimated one million Bitcoin in his possession which in April 2021 would have been worth \$65 Billion US Dollars.

Previously disproven suspects include:

- Dorian Nakamoto was coined as the founder of Bitcoin simply due to his name and previous training as an engineer. The Japanese-American man aggressively denies the claims.
- Australian Scientist and Statistician, Craig Wright whose blog posts before the creation of bitcoin raised suspicions into his involvement, but this was quickly disproven.
- Nick Szabo, the individual credited with pioneering smart contracts created BitGold before the establishment of Bitcoin.

### THE EARLY HISTORY OF BITCOIN:

- **2008:** Satoshi Nakamoto introduces Bitcoin
- **2009:** Satoshi Nakamoto mines the Genesis Block
- **2010:** The first transaction made using Bitcoin is two pizzas for 10,000 BTC
- **2011:** A Darker Side of Bitcoin History is tied to the Dark Web, and a website known as 'Silk Road' where narcotics, weapons and other illegal items are sold. Founded in 2011 by Ross William Ulbricht, the website implemented

Bitcoin as a method to process anonymous payments. Silk Road and its payment system were promoted on Bitcoin Forums and Gossip Columns, and over the next year, Bitcoin rose from \$1 to \$30

- **2013:** Bitcoin experienced its first major price spike rising above \$1000 per coin as cryptocurrencies broke into the mainstream
- **2014:** The largest Bitcoin exchange is hacked, triggering a multi-year bear market
- **2017:** Continued exposure pushes Bitcoin to its all-time-high of \$20,000



# #2 ETHEREUM

Inception: January 2014 | Supply: 116,471,411M | Max Supply: Nil



Second to Bitcoin by Market Cap is Ether. The first distinction that must be made is the difference between Ethereum and Ether. Ethereum is the global network that runs Decentralized Applications (Dapps), whereas Ether is the currency used on this platform.

The Ethereum Network was established by Vitalik Buterin in 2014. It was described as "A Next-Generation Smart Contract and Decentralized Application Platform" in its whitepaper.<sup>2</sup> The network was established with 5 key principles in mind:

- **Simplicity:** Meaning an average programmer can understand and use it.
- **Universality:** The network is accessible and viewable to anybody.
- **Modularity:** Modifications can be made, and applications added.
- **Agility:** The structure of Ethereum is editable and modifiable.
- **Non-Discrimination:** The protocol will not prevent specific practices.

The Ethereum Network achieves these principles through a platform for individuals to create and implement Decentralized Applications (Dapps).

These Decentralized Apps are programmed into the Ethereum Network using Solidity, Ethereum's own programming language. Once complete, Dapps are not owned by the writer but are publicly viewable on the blockchain and accepted by the Ethereum network. Smart contracts integrated into these apps ensure their operation by being accepted and executed by the Ethereum network.

The decentralized applications on the Ethereum network are not editable and follow the conditions they were programmed with strictly. This concept follows the quote, "code is law," meaning that the decentralized applications enforced by smart contracts are in themselves a decentralized justice system that cannot be manipulated or corrupted. The only way for the "code is law" concept to be challenged is if the entire network decides against the execution of the smart contract and collectively overrides its decision.

"The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of trade-offs that we believe will be very useful for a large class of decentralized applications, with particular emphasis on situations where rapid development time, security for small and rarely used applications, and the ability of different applications to interact efficiently, are important."<sup>1</sup>

The current Ethereum network has the capacity to process 15 transactions per second, limiting the true implementation of the network in a decentralised financial system. A more scalable network will allow Ethereum to process thousands of transactions per second.

This will be achieved through the process of Sharding, which increases the number of blockchains that store data.

The process of validating transactions will remain efficient because each node will operate on individual chains spreading the load and making nodes more efficient. The current Ethereum Blockchain will become one of these shards and will be the only shard that can store transactions. Increased security will reduce the ability for attackers to act fraudulently on the network and instil more trust in the users of Ethereum and Ether.

Ethereum was initially established using the proof of work system used by Bitcoin, where miners were rewarded with Ether by expanding computational power. Ethereum 2.0 will instead use Proof of Stake to address issues of sustainability.

To stake Ethereum, one must first have the technical knowledge to set up the stake and have a dedicated computer to operate on the network. One must also have a minimum of 32 Ethereum in a wallet connected to the network on an independent node.

Only 900 nodes per day are allowed to join the community of stakers, and the more stakers there are, the less the return on staking each Ethereum. Hence, there are a variety of barriers to entry when staking, and its benefits are slowly diminished over time.

In 2021 or 2022, Ethereum 1.0 and 2.0 will merge through an event known as The Docking. The Docking involves the Ethereum 1.0 Blockchain merging to become one of the Ethereum 2.0 Shards.



## VITALIK BUTERIN

Vitalik Buterin was born in Kolomna Russia and at the age of 21, launched the Ethereum platform. The Russian-born computer programmer studied in Canada under cryptographer Ian Goldberg, and in 2011, began writing for Bitcoin Weekly. There he was paid 5 Bitcoin per article he wrote. Thanks to his ownership of Ether, Shiba Inu, Akita and Dogelon, Vitalik has an approximate net worth of \$21 Billion (10/5/2021).



## GAVIN WOOD

English-born Gavin Wood, co created Ethereum using his Masters of Engineering (MEng) in Computer Systems and Software Engineering. Gavin Wood left the Ethereum project in 2016 and went on to create Polkadot and Kusama.

## ETHEREUM 2.0



### MORE SCALABLE

Ethereum needs to support thousands of transactions per second, to make applications faster and cheaper to use.



### MORE SECURE

Ethereum needs to be more secure. As the adoption of Ethereum grows, the protocol needs to become more secure against all forms of attack.



### MORE SUSTAINABLE

Ethereum needs to be better for the environment. Technology today requires too much computing power and energy.



# #3 TETHER

Inception: January 2009 | Supply: 65.47B | Max Supply: Nil



Though the third-largest by market capitalization, Tether stands out significantly in this list. Tether is a stable coin, which, as previously explained, is a cryptocurrency pegged to a real-world asset. Tether is pegged to the US Dollar, meaning one Tether equals one US Dollar.

Stable coins were created to negate the often highly volatile nature of cryptocurrencies due to their smaller market capitalization, and hence, higher susceptibility to movements from buy or sell orders.

Hence, Tether enables users to enjoy the decentralized nature of a cryptocurrency without having to experience its volatility. This benefit is extensively felt by those on cryptocurrency exchanges, allowing users to own more stable currencies and also make transactions between wallets or exchanges faster and cheaper.

---

As discussed previously, Trust is an essential component in maintaining a pegged currency. People must trust that their one Tether is worth one US dollar. To maintain this Trust, Tether ensures that each token is 100 percent backed by US Dollar reserves.

---

The project has, however, been subject to continued scrutiny due to its inability to provide audited financial statements confirming that the currency is actually backed by US Dollars. The only company to have audited Tether is Moore Cayman, a company based in the Caribbean.



## BROCK PIERCE

Brock Pierce is the chairman of the Bitcoin Foundation, the founder of Blockchain Capital, and over the last decade has been involved in a wide variety of cryptocurrency projects. In 2014, he established Tether, which is currently managed by the owners of Bitfinex, a Hong Kong based cryptocurrency exchange. Pierce founded Tether alongside Craig Sellars, and Reeve Collins.

## OTHER WAYS TO MAINTAIN A PEG:



A Stable Coin peg can be maintained by pre-programmed smart contracts to algorithmically manipulate the supply of coins to maintain a certain price. Essentially, this smart contract, an unbiased central bank operating under a transparent rule set.



A Stable Coin can also be pegged to another cryptocurrency which when backed by collateral, is completely viewable and transparent to the entire network. This peg might however experience the volatility that stable coins were introduced to eliminate.

# #4 BINANCE COIN

Inception: July 2017 | Supply: 153.43M | Max Supply: 170.53M



Binance Coin was founded in 2017 by Changpeng Zhao on the Ethereum Blockchain. Binance Coin was created to be the native coin of the Binance Cryptocurrency Exchange, where currently over 200 different cryptocurrencies are listed and can be traded.

At its Initial Coin Offering (ICO), all 200 million Binance coins had already been mined and given to investors. The Binance Exchange is the largest cryptocurrency exchange with volumes far in excess of any other.<sup>3</sup>

---

Binance Coin can be used for trading and to save on fees charged by the Binance Exchange. This means that the majority of Binance coins are used as utility tokens within the Binance ecosystem.

---

The success of the Binance project can be partially attributed to the Binance LaunchPad. The Binance LaunchPad is a platform for new and upcoming cryptocurrency projects looking to stimulate interest and raise capital.

Investors within the Binance ecosystem can take part in these initial coin offerings, funneling new projects and their investors through the platform. The major caveat, though, was that these offerings must be transacted in Binance Coin, raising the importance and prevalence of the coin itself.

Binance, upon its creation, committed to repurchase coins using 20% of its profits to be destroyed. These buybacks are formally recorded on the blockchain and, over time, will lead to a slow depletion of the total circulating supply. Binance has committed to repurchase coins until 50% of the total supply is destroyed. This process can be viewed in regular financial terms as a share buyback.

In 2019, Binance launched its own blockchain, where Binance coin is now transacted.



## CHANGPENG ZHAO

Changpeng Zhao used previous coding and programming experience on Wall Street to establish Binance Coin in July 2017. He currently operates as the CEO of Binance and was listed in 2018 as the third 'Wealthiest Person in Cryptocurrency' according to Forbes.





# #5 CARDANO (ADA)

Inception: September 2017 | Supply: 31.95B | Max Supply: 45B



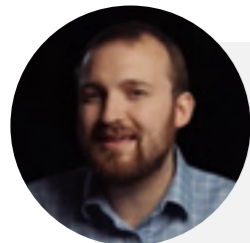
Cardano, Ada, was launched in 2017 after two years of work and is described by its whitepaper as “the first blockchain platform to evolve out of a scientific philosophy and a research-first driven approach.”<sup>4</sup> First, a clear distinction has to be made between Cardano and Ada. Cardano is a blockchain platform, whereas Ada is the currency that exists and is transacted on the Cardano Blockchain.

The coin and platform were founded by Charles Hoskinson and Jeremy Wood, two individuals who played a pivotal role in the creation of Ethereum. Hence, the two share many similarities, such as supporting smart contracts and other applications much like Ethereum.

However, Cardano is different from other cryptocurrencies as it was established using the combination of a range of peer-reviewed papers. Its intention was to improve upon the framework used across the cryptocurrency’s ecosystem and build on the inefficiencies of Bitcoin and Ethereum.

The most significant of these improvements is the use of Proof of Stake across the Cardano network and was the major cryptocurrency to do so. Unlike other cryptocurrencies, Ada uses its own unique wallet to store the currency, the Daedalus Wallet.

The Daedalus Wallet acts not only as a wallet but as an individual node on the blockchain, giving users control over their funds and access to the Cardano Blockchain. The Cardano Blockchain has a maximum supply of \$45 billion Ada coins.



## CHARLES HOSKINSON

Charles Hoskinson has a background in analytic number theory and joined the Ethereum Project with Vitalik Buterin. He left the Ethereum project following a dispute about accepting venture capital funds, and joined forces with Jeremy Wood after being approached in 2015.



## JEREMY WOOD

Jeremy Wood also worked on Ethereum with Charles Hoskinson and established the IOHK (Input Output Hong Kong), which would eventually go on to establish Cardano.

# #6 DOGECOIN

Inception: 2017 | Supply: 130B | Max Supply: Nil



The final and arguably the most intriguing cryptocurrency on this list is Dogecoin. Dogecoin was created in 2013 as a meme by Jackson Palmer and Billy Markus, as a light-hearted way to both promote cryptocurrency and blockchain technology, but also mock the extremely speculative nature of the market.

The Dogecoin logo features a Shiba Inu dog from a popular internet meme called Doge, which provides the internal monologue of the animal’s thoughts. The phrases are deliberately written in broken images. The meme itself rose to such popularity that it was mentioned by members of congress, Delta Airlines, music videos as well as on a NASCAR car.

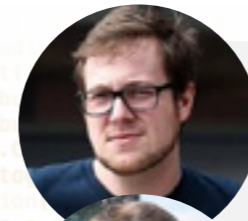
Despite its comical nature, Dogecoin operates like other prominent cryptocurrencies, using blockchain technology to allow a decentralized network of peer-to-peer transactions. Billy Markus copied many Bitcoin codes to create Dogecoin, and it shares many similarities to it. The main difference includes its supply, with 100 billion Dogecoins initially created.

Following its creation, Dogecoin rose in popularity, gaining a cult following on Reddit and became a meme in itself. In 2014, Dogecoin was used to raise \$30,000 for the Jamaican Bobsled team because they could not afford to attend the Sochi Winter Olympics. Many more charitable donations and

fundraises using Dogecoin furthered its popularity.

Despite beginning as a joke, Dogecoin went from strength to strength, eventually causing its founders, Jackson Palmer and Billy Markus, to leave the community, worried they were part of a misleading cult. In an interview with the Wall Street Journal, Billy Markus described the success of Dogecoin by saying, “It doesn’t make sense. It’s super absurd. The coin design was absurd.”<sup>5</sup> In recent years, celebrity attention has shot Dogecoin to new highs, with celebrity figures mentioning and promoting the cryptocurrency.

These include Snoop Dogg, Mark Cuban, Gene Simmons, Carole Baskin (from Tiger King) and Mia Khalifa. Arguably, its most vocal supporter has been Elon Musk through Twitter. At the beginning of 2021, Dogecoin was worth just \$0.004886, and by May, it rose to over 70 cents.



## JACKSON PALMER AND BILLY MARKUS

Jackson Palmer was born in Gosford, Australia and had no prior experience with blockchain technology. He currently does not own any Dogecoin, having given it away to charities he was promoting when the currency was worth merely nothing. Jackson partnered with Billy Markus, a software developer working for IBM in the United States, after sharing the idea of a meme coin. In 2015, he left the cryptocurrency community due to online harassment and pressure within the industry. He used his ownership in Dogecoin to purchase a used Honda Civic and also does not currently own any of the original coins.



# END NOTES

## 1 ○ THE PAST

1. What is Money, The RBA, <https://www.rba.gov.au/education/resources/explainers/pdf/what-is-money.pdf?v=2021-06-08-08-37-00>
2. Twitchett, Denis C. 1970. Financial Administration under the T'ang Dynasty. Cambridge, UK: Cambridge University Press.
3. From Chengdu to Stockholm: A Comparative Study of the Emergence of Paper Money in East and West, Niv Horesh, Page 2.
4. Ibid, Page 5

## 2 ○ THE PRESENT

1. The Federal Reserve System, Its Origin and Growth, Paul M. Warburg, 1930
2. Inflation and its measurement, The RBA, <https://www.rba.gov.au/education/resources/explainers/pdf/inflation-and-its-measurement.pdf?v=2021-06-09-13-12-26>

## 3 ○ THE FUTURE

1. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, [www.bitcoin.org](http://www.bitcoin.org), [https://www.usssc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging\\_Tech\\_Bitcoin\\_Crypto.pdf](https://www.usssc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf)
2. Blockchain Technology, Beyond Bitcoin, Berkely Engineering, 2015, <https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>
3. Proof Of Stake Vs Proof Of Work Vs Proof Of Authority, January 27, 2020, BISS Research White Papers
4. Formalizing and Securing Relationships on Public Networks, Nick Szabo, published in 1997, Satoshi Nakamoto Institute
5. Fed explores 'once in a century' bid to remake the US dollar, Politico, 2021, <https://www.politico.com/news/2021/06/12/fed-remake-us-dollar-493548>
6. Compound; Ethereum protocol <https://compound.finance/>
7. The False Narrative Of Bitcoin's Role In Illicit Activity, Hailey Lennon, 2021, <https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/?sh=2dee629d3432>

## 4 ○ THE TOP SIX

1. Ethereum Whitepaper, Vitalik Buterin, 2013, <https://ethereum.org/en/whitepaper/>
2. Ibid
3. Top Cryptocurrency Spot Exchanges, 28/6/2021, <https://coinmarketcap.com/rankings/exchanges/>
4. Cardano, Cardano documentation <https://docs.cardano.org/en/latest/?badge=latest>
5. Dogecoin's Founder Bewildered at Cryptocurrency's Sudden Popularity, February 2021, Caitlin Ostroff, <https://www.wsj.com/livecoverage/amc-gamestop-stock-market-updates/card/Cr8nEltQpzoscVrx9GRi>



