Cryptocurrency Research roughly Summarised

Getting the terms right: what is ‘digital currency’……………………………………………………..

Visualization: Taxonomy of Digital Currency………………………………………………….………….

Digital Currency before Bitcoin………………………………………………………………………….……..

How does cryptocurrency function without centralization?.........................................

Digital Signatures…………………………………………………………………..……………………..

Merkle trees………………………………………………………………………………………………….

Proof-of-Work Concept………………………………………………………………..……………..

Alternative consensus mechanisms: Proof-of-Stake…………….…………..

‘Proof-of-stake’ vs Proof of Work…………………………………………………….

Visualisation of a Bitcoin Transaction………………………......…………………………………..……

How do I obtain cryptocurrency: UK……………………………………………………………………….

Alternative Cryptocurrencies…………………………………………………………………………………..

Altcoins from 2008-2012……………………………………………………………..………………

Which Altcoins currently predominate……………………………..…………………………

Second Generation Blockchain Cryptocurrencies…………………………………………………….

What are Smart Contracts………………………………………………….……………………….

What are Decentralised Applications DApps……………………………………….………

DApp Development the current picture………………………………………………..…….

How many tokens are associated with Ethereum………………………………………..

Emerging trends associated with Cryptocurrency: Wealth Accumulation……………….

Pre-Mining……………………………………………………………….…………………………………

Initial Coin Offerings (ICOs)…………………………………… …………………………………..

Proof-of-stake validation process – the new dividend?..................................

Airdrops………………………..…………………………………………………………………………….

Emerging trends associated with Cryptocurrency: Enhanced Anonymity……………….

Private cryptocurrencies……………………………………………………………………………..

Atomic Swapping and TOR Nodes……………………………………………………………….

Darkpools……………………………………………………………………………………………………

ICOs used to launder money?.........................................................................

Glossary

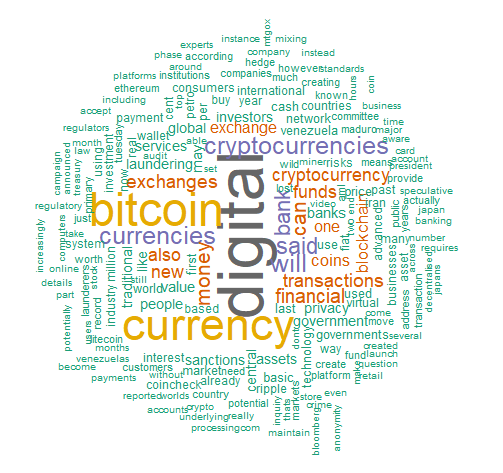
Useful Websites

Useful Books

Getting the terms right: What is Digital Currency?

If you were to look up the term ‘cryptocurrency’ you would get something like or similar to the following definition: A digital or virtual currency, that uses cryptographic encryption techniques to generate units of the currency and verify transactions. It is important to add however, that many use the term ‘digital currency’ interchangeably with ‘cryptocurrency’. Why it is important to make a distinction will be covered later, but first let’s substantiate the claim that the terms are used interchangeably.

If you were to type ‘digital currency’ into Google’s news search you would most likely receive articles about cryptocurrency and in particular Bitcoin. As can be seen below. I’ve taken the first 20 articles from google news (week of 20th feb), and taken their text using it in a word matrix. As can be seen from the matrix below ‘Bitcoin’ is the most popular topic associated with the term ‘digital’.



|  |  |
| --- | --- |
| Word | Frequency |
| Digital | 157 |
| Bitcoin | 108 |
| Currency | 103 |
| Cryptocurrencies | 49 |
| Currencies | 49 |
| Will | 49 |
| Said | 41 |
| Bank | 40 |
| Money | 37 |
| Can | 3 |

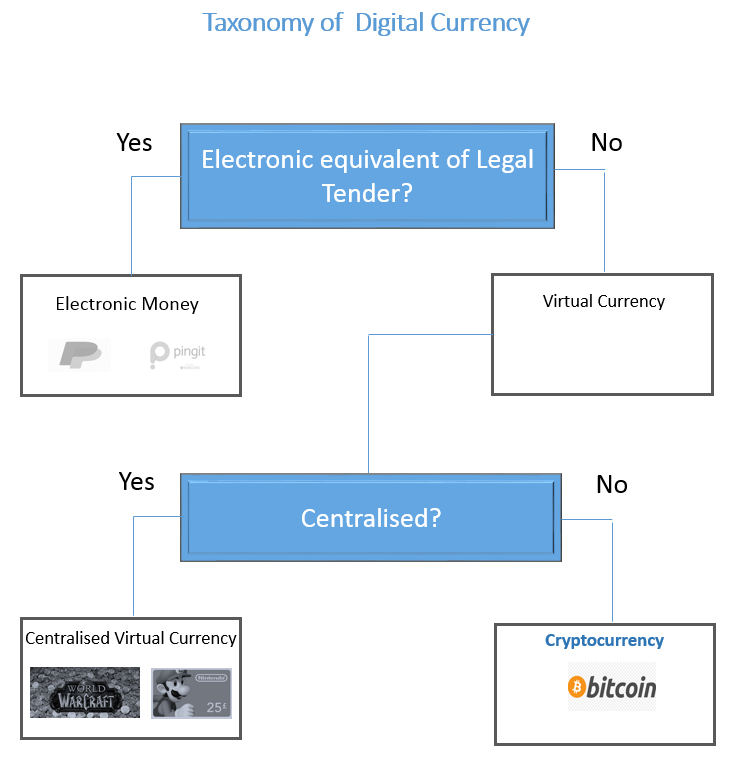
It would be very easy for anyone interested in digital currency right now to focus on Bitcoin which is actually only a tiny element of what is covered by the term ‘digital currency’. To define cryptocurrency well we first need to understand what separates it from other digital currencies.

**Digital Currency** as a broad term can contain anything that represents value in a digital manner. Digital currency can contain firstly what we would call **electronic ‘money’**, money that is simply a digital representation of government issued fiat currency. Fiat currency is government backed, so whilst it has no intrinsic value, i.e it is not tied to a commodity such as gold, it is considered legal tender.

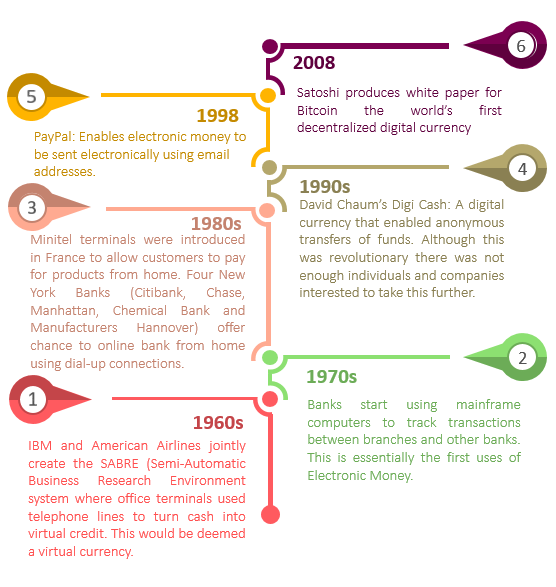
**Digital currency** can also cover **virtual currency** – electronic currency that it is not considered legal tender. Virtual currencies are controlled and created by their developers, with value being appreciated in a specific community. A prime example would be Nintendo points, users can either earn units of currency or points by completing game challenges or by exchanging fiat currency for them. Once bought, Nintendo points are only useful in the Nintendo ecosphere and seldom used elsewhere.

With the above understood, the final area of digital currency to examine is **Cryptocurrency –** a **decentralised** virtual currency. It is a virtual currency because its units are not considered legal tender, but is separate from other virtual currencies because its units are created and handled without any overseer required.

The international monetary fund and the European bank have only recently put together a taxonomy of digital currency[[1]](#footnote-1). A visual representation of how I have defined terms has been provided below.



Digital currency before Bitcoin

If we understand that Digital currency is just an electronic representation of any asset, it is useful to point out and understand that digital currency can be traced back to the 1960s. Here are the main highlights I’ve found from research:

How does cryptocurrency function without centralisation?

Bitcoin was the first digital currency that functioned without a central mediator. Before Bitcoin came about there was no way to achieve **distributed consensus** without a centralised actor. **Distributed consensus** simply means a large pool of people who are geographically segregated agreeing on something. The way that Bitcoin solved the issues of trust that made a decentralised currency impossible to achieve was the invention of the Blockchain.

What was Bitcoin’s Blockchain?

Bitcoin’s Blockchain is essentially applied three main cryptographic concepts to a single **distributed ledger (an open ledger** everyone has access to): Digital Signatures, Merkle Trees, and the cryptographic concept of Proof-of-Work.

|  |  |
| --- | --- |
| **Cryptographic tool** | **Problems (associated with decentralisation) the tool solves.** |
| Digital Signatures | Users processing transactions can instantly clarify that requested transactions are authentic |
| Merkle trees | Provides a way to chain transactions processed to each other |
| Proof-of-work | The use proof-of-work makes it extremely difficult to change the accepted chain of transactions and ensures one single chain of transactions predominates. |

**Digital Signatures**

**Digital signatures** ensure that all transactions on the network are authentic. Every transaction will be encrypted with the signing key can only be decrypted with the verification key. Digital signatures are applied so that every transaction has a unique signature that could only be achieved with a private key. A useful to [think of it](https://bitcoin.stackexchange.com/questions/19950/how-are-public-and-private-keys-related-to-the-wallet), is when someone makes a transaction to an address he/she essentially states that ‘I give the right to spend this money to the person who owns the private key corresponding to this address’. The person who has received this transaction will in turn be able to spend the transaction by signing the transaction using his private key. With this signature, he can prove that he owns the key, without even disclosing it. Others can verify the signature using the public key.”

**Merkle Trees**

Merkle trees provide a way to chain together groups of authenticated transactions. Merkle trees ensure this by utilizing the technique of hashing. Hashing is the transformation of string of characters into a usually shorter fixed-length value or key that represents the original string. Each block is chained to the preceding block by containing a hash that could only be generated using the previous block’s hash. For this reason, Merkle trees are often also referred to as **Hash trees.** [**Here**](https://www.youtube.com/watch?v=-SMliFtoPn8) **is a useful video tutorial of this**.



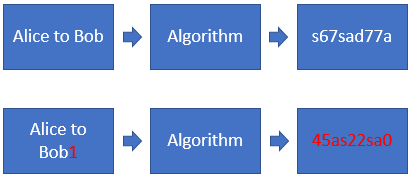
We can see that the smallest change in the message will drastically alter the resulting hash. Merkle trees work by using hashes to create a chain, where a block of data can only be added by using the previous hash. If one block is changed then the rest of the blocks will be changed. This is visually represented below. Numbers have been used instead of actual hashes for clarity.



**Proof-of-Work concept**

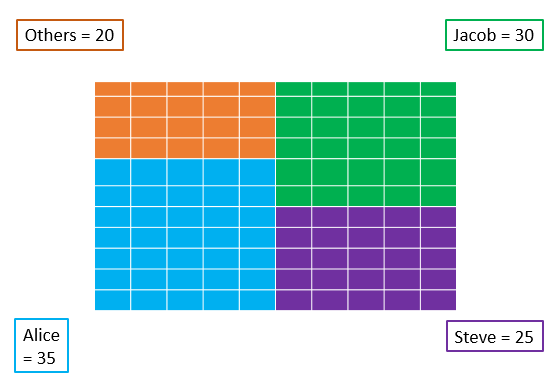
The first two cryptographic techniques have ensured that every transaction requested to added to the ledger is authentic and there is a way to order the transactions into blocks. However, if the Bitcoin creators left things here it would still be chaos. There wouldn’t be a way of agreeing which chain of blocks to choose to summarize all transactions, there would lots of different versions emerging. This is where proof-of-work comes in. Proof-of-work ensures that each block added takes time to ensure that there is order and one single chain of blocks. Users dedicating time to process transactions they are rewarded units of currency.

What is exactly this proof-of-work? Essentially for each block to be added to the chain it needs to undergo a validation process that involves solving a puzzle. Each block starts with a default hash, this is the block is put through a function that turns it into a set string of unintelligible data as explained earlier. Users wishing to earn the Bitcoin reward need to add other characters to the block until the resulting hash starts in a certain number of zeros (currently 18). This difficulty (more zeros required) is enhanced every time 2016 blocks are added to the chain. The diagram below shows that with just one character change



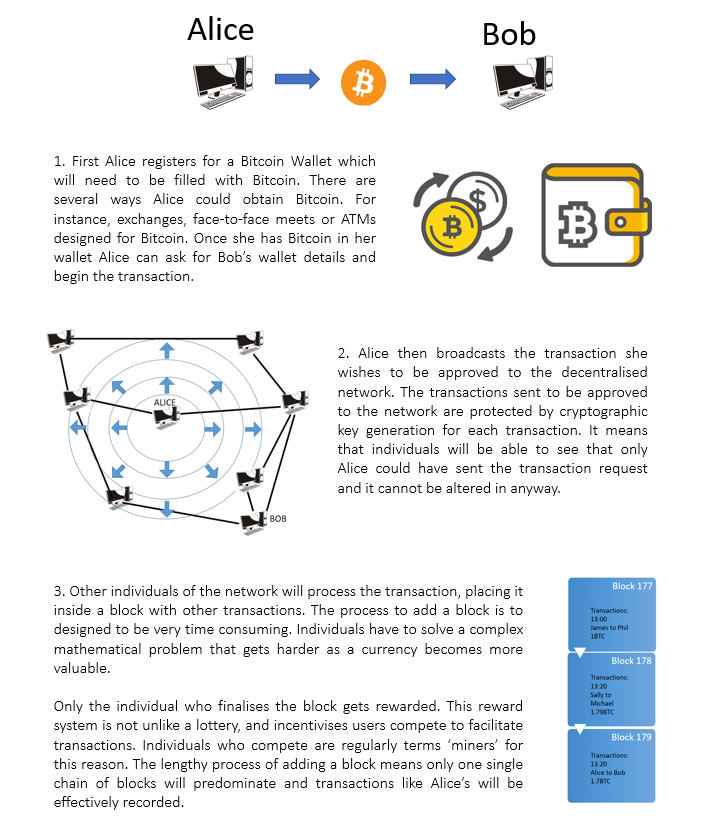
Alternative mechanisms to achieve distrusted consensus: Proof-of-stake

Proof work functions in a way that the more computational power you have the more likely you are to add a block to the chain. Proof-of-Stake functions in a way that the more wealth you stake towards the effort of adding blocks to the chain the more likely you are to win the block reward. In proof of work you will win a certain amount for instance 12.5 Bitcoin or 6 Ether. In proof-of-stake you will tend to win transaction fees. In the visual scenario below we can see that Alice would have the best chance of winning the block reward as see has largest proportion of cryptocurrency.



Proof-of-Work versus Proof-of-Stake Summarized

|  |  |  |
| --- | --- | --- |
| **Issue** | **Proof-of-Work** | **Proof-of-Stake** |
| Safety issues? | Tried and tested, so far there has not been a 50+1 attack on major cryptocurrencies. | Still yet to be adopted by a major cryptocurrency. |
| Energy consumption | Vitalik Buterin has stated that £1 Million worth of electricity is consumed per day just to mine Bitcoin and Ethereum. | No superfluous energy required |
| Transaction processing time | Tends to be Slower | Tends to be Faster |
| Knowledge required to participate | Need to know what tools are best suited to your computer competitive | No special computer knowledge required just wealth. |
| Democratic? | Mining pools dominate | Most wealthy dominate |

If the above seems to technical here demonstration of transaction using Bitcoin where technical terms have been taken out. It shows how Alice would go about transferring Bitcoin to Bob.

How do I obtain cryptocurrency in the United Kingdom?

Exchanges

By far the easiest method to obtain cryptocurrency is by going through an online exchange. Exchanges essentially allow individuals to exchange fiat currency such as Great British Pounds or US Dollars into Cryptocurrencies such as Bitcoin. Some Exchanges also allow individuals to exchange cryptocurrencies for other cryptocurrencies. For instance, Trading the most popular cryptocurrency Bitcoin for the second most popular cryptocurrency Ethereum.

There are currently 130 Cryptocurrency Exchanges on the World Wide Web. If we look at [trades by minute](https://data.bitcoinity.org/markets/volume/6m?c=e&t=b) the US based Coinbase exchange processed the most trades by minute (22% of total cryptocurrency trades per minute). CEX an exchange based in London has made the top ten with 3% of trade made per minute going being processed with its services.

Bitcoin ATMs

A popular yet less common alternative to buying cryptocurrency is through designated cryptocurrency automatic teller machines (ATMs). There are a total of 103 cryptocurrency ATMS in the United Kingdom.77 ATMS of which are in London, 6 in Birmingham 20 in other cities with just a few ATMS each.

Bitcoin Meetups

Another way to get hold of cryptocurrency is to go to meetups where cryptocurrency can be bought from individuals in person. For instance, on meetup.com an individual could search for events held in their area or nearby that facilitates a meetup for trades.  Websites like localbit.com also allow for individuals to buy and sell Bitcoin in person. Individuals can list how much they are willing to sell and their preferred method of payment.

Mining for Bitcoin

Mining is the process by which individuals on a cryptocurrency network work to process cryptocurrency transactions. They are rewarded with cryptocurrency for their efforts. Popular cryptocurrencies like Bitcoin and Ethereum would be extremely difficult for a sole individual to process as they are competing against a huge amount of computer power. In fact some have estimated that mining for Bitcoin uses over 42TWh of electricity in a year, which places its energy consumption higher than [New Zealand and Hungary.](https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency) This said, mining can still be accomplished by an individual by joining a mining pool – a group of users combining their computing power and sharing the proceeds if they win the reward of processing a block of transactions.

Alternative Cryptocurrencies

As Bitcoin’s source code is openly available, it means developers easily build on it to create their own alternative cryptocurrencies or ‘altcoins’. Many popular cryptocurrencies can be traced back to a major cryptocurrency before. For instance, the cryptocurrency Dogecoin, was a variant of Litecoin, which was a variant of Bitcoin.



If we analyze the very first altcoins we can see that there were only small changes made to Bitcoin’s original source code. Altcoins tended to differentiate in a few aspects. Firstly, the amount of coins that could be produced, the speed at which transactions were processed and the reward given to those facilitating transactions. Below is a summary of the first altcoins to be produced. Most are directly linked, with little in the way of major differences.

Altcoins from 2008-2012

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Father Coin?** | **Unique Features** |
| Namecoin | Apr 2011 | Bitcoin | Namecoin uses cryptographic tokens similar to Bitcoin to bitcoins to authenticate ownership of ‘.bit’ domains. |
| iXcoin | Aug 2011 | Bitcoin | Essentially Bitcoin but a reward of 96 coins per block added to the chain but the same 21 million coin limit. |
| I0coin | Aug 2011 | I0Coin | Updated version of iXcoin that requires less memory. Storing iXcoin used about 8.2 GB of memory, I0 Coin needs just 250MB. |
| SolidCoin | Aug 2011 | Bitcoin | Aimed to offer faster transaction processing that Bitcoin (3 minutes per block). |
| Geist Geld | Sep 2011 | Bitcoin | Simply an experiment on the Bitcoin algorithm to see how fast it could go. |
| Tenebrix | Sep 2011 | Geist Geld | Began testing using a hashing algorithm separate to Bitcoin’s SHA256. Uses ‘Scrypt’ instead. |
| FairBrix | Oct 2011 | Tenebrix | Main difference is that Fairbrix does not come with 7.7 million reserved by the creators |
| Litecoin | Oct 2011 | Bitcoin | Unlike the proceeding currencies it has a cap on coins to stop inflation. Transaction time of 2.5 minutes. |
| Liquid Coin | Jan 2012 | Litecoin | Block reward reduces at 4% per block and never increases |
| Devcoin | Feb 2012 | Bitcoin | 90% of the Devcoin coins go to open sources projects. |
| Anoncoin | June 2012 | Litecoin | A coin with I2P Support. I2P is an anonymous network layer. |
| Freicoin | June 2012 | Bitcoin | Applies a continuously-assessed fee to all accounts, and distribute the proceeds to miners. |
| BBQCoin | Jul 2012 | Litecoin | Coin made not to be sold or traded – just for fun. A 51% attack made the currency weak. |
| Peercoin | Aug 2012 | Bitcoin | Proof of stake/proof-of-work hybrid system. |
| Terracoin | Oct 2012 | Bitcoin | Block every 2 minutes, 42 million coins available, difficulty adjustment 30 blocks, 20 coins per block. |
| Novacoin | Nov 2012 | Peercoin | It cuts rewards achieved by miners in half every 64 blocks as opposed to Peercoin’s 16 blocks. |

There are now thousands of cryptocurrencies listed on websites like coinmarketcap.com. What has caused this explosion? For one as the cryptocurrency ecosphere is dedicated to open source development competent developers now have a host of other cryptocurrencies to build on. Secondly, cryptocurrencies like Ethereum make it relatively easy to create applications and altcoin on top of its blockchain. As of March (28th) 2018 there are currently 1591 total cryptocurrencies listed on coinmarketcap website.

|  |  |
| --- | --- |
| **Year** | **Number of Cryptocurrencies** |
| 2008 | 1 |
| 2011 | 9 |
| 2012 | 17 |
| 2013 | 197 |
| 2014 | 646 |
| 2015 | 667 |
| 2017 | 1000+ |
| March 2018 | 1591 |

Which altcoins currently predominate?

Here is the market capitalization at March 28th 2018 16:00.

|  |  |  |
| --- | --- | --- |
| **Cryptocurrency** | **Price** | **Market Capitalisation** |
| Bitcoin | $7,942.32 | $134,577,743,758.00 |
| Ethereum | $451.27 | $44,435,714,749.00 |
| Ripple | $0.58 | $22,493,723,749.00 |
| Bitcoin Cash | $876.68 | $14,940,812,816.00 |
| Litecoin | $133.96 | $7,478,711,420.00 |
| EOS | $ 6.17 | $4,669,393,748.00 |
| Cardano | $0.16 | $4,108,455,452.00 |
| Stellar | $ 0.22 | $4,049,909,665.00 |
| NEO | $57.09 | $3,711,097,000.00 |
| IOTA | $1.20 | $3,331,378,225.00 |

The top ten cryptocurrencies differ from each other, but can be grouped together in the qualities they share. Starting from Bitcoin as a core cryptocurrency a quick summary is offered here:

Bitcoin cash and Litecoin function in the same way as Bitcoin except their adoption rates differ. Litecoin was designed so that transactions could be processed quicker and has a different supply limited to Bitcoin as covered earlier. Bitcoin Cash is essentially Bitcoin but with eight times the scalability. It was a **hard fork** of Bitcoin where one camp decided to create an entirely new cryptocurrency because of how to deal with the scalability issues (current protocol cannot cope with the amount of transactions being processed).

Two of these, Ripple and Stellar, differ from above in that they are designed as transaction networks. Most digital currencies are designed to be stored unit of value however Ripple and Stellar are created to digitalize regular fiat (national currency) transactions with their tokens. Both digital currencies offer faster payment solutions by utilizing blockchain technology. Ripple is suited towards banks and stellar for individuals trading foreign currencies. Both have central interference on what transactions are processed so it would be difficult to call them pure ‘cryptocurrencies’.

The rest of the cryptocurrencies in the top ten can be considered much more than a store of value or a payments processing service. Ethereum, EOS, Cardano, NEO and IOTA all offer the ability for users to build on top of them. Instead of just being a currency, they have been designed to be built on top of. Ethereum was the first cryptocurrency designed specifically to make building applications on top of a blockchain easy. The others above essentially enable individuals to do the same but differ from Ethereum in several aspects. Here is a good article explaining the pros and cons of each [decentralized platform](https://coincentral.com/best-dapps-platform/)

Second Generation Blockchain Cryptocurrencies

Cryptocurrencies that enable smart contracts and decentralized applications to easily be constructed are often called [‘second generation’](https://steemit.com/bitshares/@heiditravels/blockchain-generations-from-bitcoin-to-smart-contracts-and-graphene) cryptocurrencies. Whilst there were a few smart contracts built on top of Bitcoin such Mastercoin (now Omni) and Coloured Coins these were difficult to build. Ethereum made smart contracts much easier to build by constructing a completely unique language that could be easily integrated with its purpose-built platform. Essentially Ethereum made it easily possible to add updated details of ongoing smart contracts or add new smart contract details into blocks with transactions simultaneously being processed on the network. Ethereum is far by most commonly used platform to build a variety of different decentralized applications.

What are smart contracts?

A smart contract is a piece of code that implements arbitrary rules. A useful way of thinking about smart contracts is just to realise that smart contracts are essentially the same as contracts - with the difference that they will automatically execute any actions that parties involved have agreed.

Let’s use Vitalik Buterin’s (creator of Ethereum) [scenario](https://github.com/ethereum/wiki/wiki/White-Paper) to explain what a smart contract is:

* Let’s say A wants to pay B $500 to build a website
* Contract agreement: A puts $500 into the contract, funds are locked.
* B finishes website and sends a message to the contract asking to unlock the funds
* If A agrees funds are released.
* If B decides to not finish the website B can quit by sending a message to relinquish funds.
* If A and B disagree it will be up to a defined judge (both A and B agree on who this is at the start) to decide.

In Vitalik’s [own words](https://www.youtube.com/watch?v=66SaEDzlmP4):

The “basic concept [of a smart contract] is if you have some new kind of application what you would do is write the rules of your application in a piece of code… Take this piece of code you would call this a contract”. Once you’ve uploaded this to the blockchain you have a special type of account that is essentially controlled by the code you have written. The moment you send one ether to that account you relinquish control of that account and no one controls it anymore – it is essentially a robot that sits on top of the blockchain.

What are Decentralised Applications (DApps)?

Let’s start with what an application is. An application is piece of software designed for a specific purpose. Microsoft PowerPoint for instance is an application that allows you to create slideshows for presentations. A decentralized application is just an application that does not have a no single point of information to run the application. For instance, a web App like Facebook will have a central server to connect to. Whereas any app built on Ethereum’s blockchain will be run through the smart contracts designed to run it. There is no agreed definite definition of what a DApp is but there is a broad consensus on what the three main characteristics are for DApps involving monetary value.

Firstly a DApp tends to be **Open Source:** A DApp is characterized by its transparent nature. Open source means that anyone can see the code that was used to build the DApp. Secondly a DApp has **Internal Currency or Tokens**: Because decentralised apps are open sourced charging users for the service would be fruitless. The answer is to allocate scare resources in the network by using a scarce token. Owners of scare resources get paid in unit’s native to the DApp. As the DApp becomes bigger and more used these scarce resources become more valuable. Thirdly a DApp will have a **Mechanism to achieve decentralized consensus:** As there is no single entity controlling the application, distributed consensus needs to be achieved without trust. For this reason, Bitcoin can be considered one of the first monetary DApps as well as the first cryptocurrency.

DApp Development: The current Picture

As mentioned earlier the main reason that many DApps are built with Ethereum is because it was the first to implement a unique code to enable widespread adoption of them. With Smart Contracts, Ethereum has made it easy for DApp developers to create their own tokens to fuel their DApps. The ERC20 token standard developed in 2015 defines a common list of rules that an Ethereum token has to implement. Ethereum’s protocol has become very popular with [crowdfunding companies](https://medium.com/blockchannel/understanding-the-ethereum-ico-token-hype-429481278f45). Ethereum even provides its own guide that shows you how to use smart contracts to create a token – mentioning at the end that they are very useful for crowd sales [www.ethereum.org/token](http://www.ethereum.org/token).

How many Tokens are associated with Ethereum?

As of January 2018, there were more than 21,000 ERC20 token contracts. The most successful of these tokens are listed on www.coinmarketcap.com where there are a total of 476 tokens that were built on the Ethereum blockchain. Data taken from www.coinmarketcap.com would indicate that these tokens have a current market capitalization of over 42 Billion Dollars (as of 21/02). As a platform where individuals can build tokens Ethereum far is the largest. But others do indeed exist, no doubt due to the success of Ethereum. Omni for instance has 2 Billion worth in market capitalization and NEO has 738 million dollars. Ethereum dominance as a token platform is demonstrated below.

Top ten Ethereum Tokens (21/02/2018)

|  |  |  |  |
| --- | --- | --- | --- |
| **Code** | **Token Name** | **Description** | **Market Cap** |
| EOS | EOS.IO | Infrastructure for decentralised applications. **Despite launching these tokens EOS will be released on a completely different blockchain.** | $6,172,324,185 |
| TRX | TRON | TRON is an application intended to allow content creators to be compensated for sharing their content. | $3,053,977,241 |
| VEN | VeChain | Blockchain-as-a-Service company with a mission to build a trust-free and distributed business ecosystem to enable transparent information flow, efficient collaboration, and **high-speed value transferring.** | $2,941,319,037 |
| OMG | OmiseGo | OmiseGo aims to become the number one peer-to-peer cryptocurrency exchange system. Aims to offer cryptocurrency users an alternative to online exchanges. | $1,917,287,709 |
| ICX | ICON | Wants to “hyper connect the world” by building one of the largest decentralised networks in the world. It is building a platform that will allow various blockchains to interact with each other via smart contracts. | $1,614,402,246 |
| BNB | Binance Coin | Trading platform exclusively for cryptocurrencies: Crypto-to-Crypto. | $974,212,608 |
| PPT | Populus | Intends to become a platform for peer-to-peer invoices. | $895,508,552 |
| RHOC | Rchain | A new type of blockchain technology. It claims to provide content delivery at the scale of Facebook and process transactions at the speed of visa. | $835,089,650 |
| SNT | Status | Mobile operating system of Ethereum. | $703,276,187 |
| MKR | Maker | A stablecoin (no volatility) 1 Dai = One Dollar. | $650,585,812 |

Risks associated with the proliferation of cryptocurrencies: Wealth Accumulation

The first major trend I have identified whilst researching cryptocurrency, is that cryptocurrencies are providing new ways for wealth accumulation.

Pre-mining: What is it?

Pre-mining is essentially taking units of a soon to be released cryptocurrency by mining them before the cryptocurrency is launched publicly. If the cryptocurrency is successful, the owner(s) who created the cryptocurrency can accumulate wealth at a staggering rate. Just by mining the first block, the ‘Genesis Block’ Satoshi Nakamoto would have earned 50 BTC, which is now equivalent to £335,472.30. In fact, because Bitcoin was hardly used outside of the computer science community in the early years it is advocated that the creator could have mined the equivalent of 1 million BTC which would currently equate to £6,709,445,980.45.

*Okay but that’s Bitcoin, what other cryptocurrencies have the capability to do that?*

Let’s look at Ethereum: Ethereum creators pre-mined 60 million units of their cryptocurrency for the Initial Coin Offering and **kept 12million** for themselves.

Within a year of Ethereum being released, with Ethereum trading at $11.80 on July 1st 2016, the creators held $141,600,000 worth of Ethereum.

Although this wealth accumulation is based on virtual currency it does beg the question of what government involvement there should be. Because virtual wealth **can** and is converted back to fiat currency. If a cryptocurrency is garnering a lot of attention, you can bet that the owners will become instantly rich when it is released by investors. Considering the explosion of cryptocurrencies, and the constant changing picture of the big players it would be certainly worth paying attention to the pre-mined rate of new cryptocurrencies.

Initial Coin Offerings: What are they?

An Initial Coin Offering is very similar to an Initial Public Offering. Initial coin offerings are used to fundraise a cryptocurrency project. The public are promised tokens or units of the cryptocurrency in return for funding the project. There is a funding goal that the Initial Coin Offering has to attain. If it meets this, then the project will go on, if it doesn’t then investors will have their contributions to the project returned.

The Ethereum foundation produced a technical framework that could be used to finally manage a larger number of investors and supporters in a transparent automated and simple way.

To date approximately [$168,000,000](https://blog.bitaccess.co/key-trends-in-the-ico-market/) has been contributed through Initial Coin Offerings (ICO) to new cryptocurrency creators. Considering that from 2013 to 2017 the majority of ICOs have completely failed with participants losing of their money. Please see the [mangrove report](http://www.mangrove.vc/ico-report2017) to get a better understanding.

[Bitcoin.com](https://news.bitcoin.com/46-last-years-icos-failed-already/) using tokendata.io’s data has indicated that of the 902 crowd sales that took place last year 142 failed at the funding stage and 276 have since failed, either due to taking the money and vanishing or slowly fading away. An additional 113 ICOs can be classed as semi failed as their team has stopped communicating through social media. In total this means that 59% of last year’s crowd sales were confirmed as failures. These projects still raised $233 million between them.

There does seem to be an over eagerness to be part of the emerging cryptocurrency scene. The United States Commodity Futures Trading Commission has recently warned of the current craze advising [against](https://www.cnbc.com/2018/02/15/u-s-regulator-warns-of-pump-and-dump-cryptocurrency-frauds.html) buying into ICO tokens from social media tips.

It does not seem to be hard to generate a lot of money from the hype. A proposed ICO simply needs a website filled with cryptocurrency related jargon, a proposed roadmap and development team. In fact, ICOs are making money without the aforementioned even being true. Take this ludicrous example. ‘[Miroskii’](https://miroskii.org/) an ICO for a cryptocurrency aim to ease the difficulty associated with financial transactions. In Early March the development team listed contained pictures of Ryan Gosling as [a lead developer](https://www.independent.co.uk/life-style/gadgets-and-tech/news/ryan-gosling-cryptocurrency-scam-miroskii-kevin-belanger-stock-image-fake-profile-bitcoin-a8240386.html). It has since claimed that it was hacked by Russians. Even if this claim is true it is staggering that whilst the company had Ryan Gosling listed as a lead developer it still generated $830,000 in crowdfunding.

Another example was in Mid-February, a New York Based company changed its name from the Long Island Iced Tea Corp to Long Island Blockchain Corp and its publically listed stock jumped 200 percent. Whilst the majority of ICOs are scams it is clear many people are making a lot of money out of ICOs, because it is cryptocurrency regulators need to ask themselves is it worth paying more attention to the creators of ICOs.

Proof-of-stake validation process – the new dividend?

Now that cryptocurrencies are implementing proof of stake consensus methods individuals without large quantities of cryptocurrency are now able to collect interest just by holding their units in place. Ethereum the world’s second largest cryptocurrency is incorporating proof of stake. As Dana Edwards mentions the holy grail of investing ‘compound interest’ has now made its way to cryptocurrency – particularly now that a valuable cryptocurrency like Ethereum has adopted [proof of stake:](https://steemit.com/ethereum/@dana-edwards/proof-of-stake-casper-ether-and-compound-interest-gains)

**“If Proof of Stake (Casper) is a success there may be no reason to cash out into fiat any more than is necessary to self-sustain”**

“In a sense, these ETH tokens could become exponentially more valuable than they are today. $100 per ETH today is meaningless if ETH start paying 8% interest in the form of Proof of Stake. The incentives currently are to cash out only as much as necessary to live because of 40% income taxes, as well as capital gains taxes, etc. In a situation where there is 8% interest on the equivalent of 1 million dollars in wealth, this would mean large crowdsale Ethereum stakeholders might never in their lives exhaust their stakes and simply live off the interest indefinitely. If developers are among these individuals then the developers will in a sense be "set for life" off 8% stake assuming Ethereum is a success and continues growing with their help. For this reason, developers and stakeholders will have every reason to expand the pie, continue to grow Ethereum, and maintain it.”

I have found a few examples [here](https://steemit.com/cryptocurrency/@michellerhey/how-to-make-money-with-cryptocurrency-proof-of-stake-coins) and [here](https://steemit.com/crypto/@billionairebit/earning-passive-income-via-proof-of-stake-pos-coins) that show that theoretically making money through proof-of-stake mining is becoming a trend for alternative cryptocurrencies too. Too make it more likely that you will earn rewards buying masternodes is also an emerging trend. I have found the following websites that will allow users to buy masternodes: <https://masternodes.online/> and <https://masternodes.pro/>.

Airdrops

Another emerging trend are ‘airdrops’. Airdrops are when a blockchain project distributes free tokens or coins to cryptocurrency users. Often to be a recipient of an airdrop users often only need coins of a specific cryptocurrency stored in your wallet. For instance, users of Byteball, Stellar Lumens and OmiseGo have all had cryptocurrency dropped into their wallet free. Other airdrops may require a user to make social media posts or to talk to a member of a team on bitcointalk.com.

Here is a description taken from <https://airdropalert.com>:

‘The​ ​format​ ​of​ ​these​ crypto ​giveaways​ ​is​ ​usually​ ​like​ ​this:​ ​At​ ​a​ ​pre-announced​ ​time​ ​the​ ​project​ ​behind the​ ​event​ ​will​ ​take​ ​a​ ​”snapshot” ​of​ ​the​ ​blockchain,​ ​and​ ​anyone​ ​holding​ ​Ether or Bitcoin​ ​at​ ​that​ ​point​ ​will​ ​receive​ ​a certain number​ ​of​ ​free​ ​tokens.​ ​This can also be done on other blockchains, but Ethereum and Bitcoin are the most used for this airdrop format.

Another possible way to get free crypto is a faucet. This means you get a small amount of free crypto for a longer period of time. An example of this one is a crypto wallet that drops Bitcoin, NEO, Litecoin, Dash & more every day, [click here](https://qoinpro.com/2102282481bb40bf04cc7708447267e8) to check this out”

Emerging Trends Associated with Cryptocurrency: Enhanced Anonymity…………………………….

There has been a lot of attention on Bitcoin and its perceived role in enabling criminals to transfer units of cryptocurrency anonymously. Whilst it is difficult to attribute a public key an individual unless records are available – transactions on a blockchain like Bitcoin are transparent. In fact, every single transaction that has been verified is accessible via Bitcoin’s blockchain. [Here](http://anonymity-in-bitcoin.blogspot.co.uk/2011/07/bitcoin-is-not-anonymous.html) is a useful article detailing how you can trace and analyse bitcoin transactions. In fact, anyone is free to download Bitcoin’s block chain [here](https://bitcoin.org/en/download) it is currently a 145GB download. This means if you have knowledge of an individual’s public key address, you can see the transactions he/she is making. It is for reasons like this that individuals have created cryptocurrencies that mask their blockchain/public ledger. We will now turn focus to these more ‘cryptic’ cryptocurrencies.

Private currencies

There are cryptocurrencies that will that go provide much deeper levels of anonymity than bitcoin. When researching this, I believed the list to be under ten, but further searching would reveal there are at least [35 cryptocurrencies](https://www.reddit.com/r/CryptoCurrency/comments/7lxq79/full_list_of_privacy_coins_networks/) that could be considered ‘private’. Private in this sense means transactions are either difficult to trace to a user or are completely anonymous. Probably the most common way to obscure transactions, because it is commonly used with Bitcoin, is through mixing. Coin mixing essentially adds a layer of anonymity to transactions through sending smaller proportions of your intended payment in several wallets. With Bitcoin, individuals wishing to mix coins can set up a scheme with others to achieve this such as <https://coinmixer.se/en/>. With DASH this comes built in, with masternodes providing the coordination required to mix coins.

Other privacy based cryptocurrencies either use the ‘cryptonote’ protocol or the zero-knowledge protocol called Zk-snark (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). The cryptonote protocol very briefly explained makes transactions hard to read utilizing the use of cryptographic technologies such as ring signatures and stealth addresses. This means that for every transaction there could be multiple receivers and senders which are equiprobable. Zero knowledge proofs work by providing the option to ‘mint’ new untraceable coins. Minted coins are then mixed with other minted coins. When a user wants to send a unit of the currency to another user, it will be a random coin picked at random meaning no one can trace it back to original sender.

Here I have provided the top ten according to a coinmarketcap rating:

|  |  |
| --- | --- |
| **Name** | **Coinmarket rank** |
| Dash | 11 |
| Monero | 12 |
| Zcash | 24 |
| Bytecoin | 29 |
| Verge | 31 |
| Komodo | 46 |
| Aion | 50 |
| Hcash | 51 |
| PIVX | 57 |
| Electroneum | 59 |

Atomic Swapping and TOR Nodes

Two trends interested me when I analysed the top ten looking for trends that I did not know. One is the implantation of TOR nodes into cryptocurrencies. This is for instance the case with the Cryptocurrency Verge. Verge has adopted a different approach to approaching the issue of privacy. Unlike other popular privacy based cryptocurrencies that use methods from cryptography to make their blockchain harder to read, Verge uses TOR and I2P network to make the IP addresses of individuals impossible to read.

Another is the implementation of private cryptocurrencies enabling ‘atomic swapping’ both Verge, as just discussed, and Komodo enable users to switch cryptocurrencies for other cryptocurrencies without going through an exchanger or intermediary. This means that criminals around the world may have another way of evading an overseer. Even if governments around the world had access to the most popular exchanges given an individual already has some cryptocurrency they can trade it for other cryptocurrencies freely. However atomic swapping is not the only method of exchanging cryptocurrencies for other cryptocurrencies and fiat currency there are also dark pools and increasing smart contracts that are a cause for concern to authorities around the world.

Darkpools

Dark pools are used to enable investors wanting to trade in large quantities to do so outside standard exchanges. This is done to ensure no effect is made on the price of the asset they are trading. When applied to cryptocurrency there are two main differences.

Firstly, as mentioned above dark pools are above to conduct trades utilizing atomic swaps i.e one cryptocurrency for another. Second, the execution as [Investopedia](https://www.investopedia.com/news/number-dark-pools-cryptocurrency-trading-increasing/) points out is different. Instead of a direct matching, some darkpools ([Republic Protocol](https://medium.com/research-center/republic-protocol-ren-ico-analysis-a-decentralized-dark-pool-for-cryptocurrency-assets-e20bc125d3bf) for instance) can match a large order with several individuals looking to sell through a matching engine known as Multiparty Computation Protocol (MCP). [Kraken](https://blog.kraken.com/post/259/introducing-the-kraken-dark-pool/) is also offering its uses a service to trade cryptocurrencies in large quantities off the standard exchange.

Peer to peer trading provided by smart contracts

**Ethereum Smart contracts are now being designed to allow individuals to trade peer2peer without going through an exchange.** [**www.localethereum.com**](http://www.localethereum.com)**. This shows the potential to use** smart contracts as a method to launder money. It would be easy to list a bespoke listing to sell either illicitly gained Ethereum or fiat currency.

ICOs used to launder money?

Initial coin offerings as well as offering an ability for criminals to set up scams as outlined in the section above also offer a new way of ‘transaction laundering’. Transaction laundering is essentially when you list a product for sale on the internet and get someone you know to pay for it. In the past, this has been done on eBay using ‘black Disney videos’ – videos that a listed at particularly high prices that no-one other than the other criminal will buy. Tokens also present this possibility. Criminals could set up an ICOs just to transfer funds. Worthless tokens could be sent in return for ether that could then be exchanged. With the emergence of darkpools a criminal could transfer large amounts of ether at once to fiat currency.

Glossary:

Soft fork – A soft fork is a change to the software protocol where only previously valid blocks/transactions are made invalid. Since old nodes will recognize the new blocks as valid, a softfork is backward-compatible. This kind of fork requires only a majority of the miners upgrading to enfire the new rules, as opposed to a hard fork.

Hard fork – A change to the software protocol where all nodes need to update and agree on to continue to use the cryptocurrency.

Software fork – Someone takes original code and modifies it in order to create a new cryptocurrency of their own.

Public key cryptography: Public Key cryptography allows you to hand people a public key and use the corresponding private key to prove ownership. You can create any random private key (keeping it secret) and calculate the corresponding public key (give it out for verification). Using this private key, you can sign a message and other people can verify that you own the private key by using your public key.

Useful websites:

<http://cryptoslate.com/about> --> gives a nice overall picture of the cryptocurrency market space.

[www.tokendata.io](http://www.tokendata.io) 🡪 up to date information on token sales.

1. See the following reports [IMF](https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf) (2016) Virtual Currencies and Beyond and the [European Central Bank](https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf) (2015) Virtual Currency Schemes a further analysis. [↑](#footnote-ref-1)