SIGMA CAPITAL ADIVISORS LLC

Cryptocurrencies – A Premier Overview

1. Description

A cryptocurrency (or altcurrency) is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies.

The first widely used crypto currency is Bitcoin which is a type of virtual currency that is secured by cryptographic encoding and can only be sent or received using a public key, by the owners of the private keys necessary to unlock its value.

Users can transfer bitcoin, using a virtual (online or offline) wallet, over the network to do just about anything that can be done with conventional currencies, including buy and sell goods, send money to people or organizations, or extend credit. Most altcurrencies can be purchased, sold, and exchanged for other currencies at specialized currency exchanges. The appeal for these altcurrencies is growing as people find them (especially Bitcoin) to be a fast, secure, and borderless way to transact.

Bitcoin's main innovation and advantage is that it works on a distributed, peer-to-peer system, called a Blockchain (a distributed decentralized ledger). As such there is no central server or point of control. Bitcoins are created through a process called "mining," which involves competing to find solutions to a mathematical problem (or algorithms) while processing bitcoin transactions. Every 10 minutes, on average, a bitcoin miner is able to validate the transactions of the past 10 minutes and is rewarded with brand new bitcoin. Essentially, bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central bank.

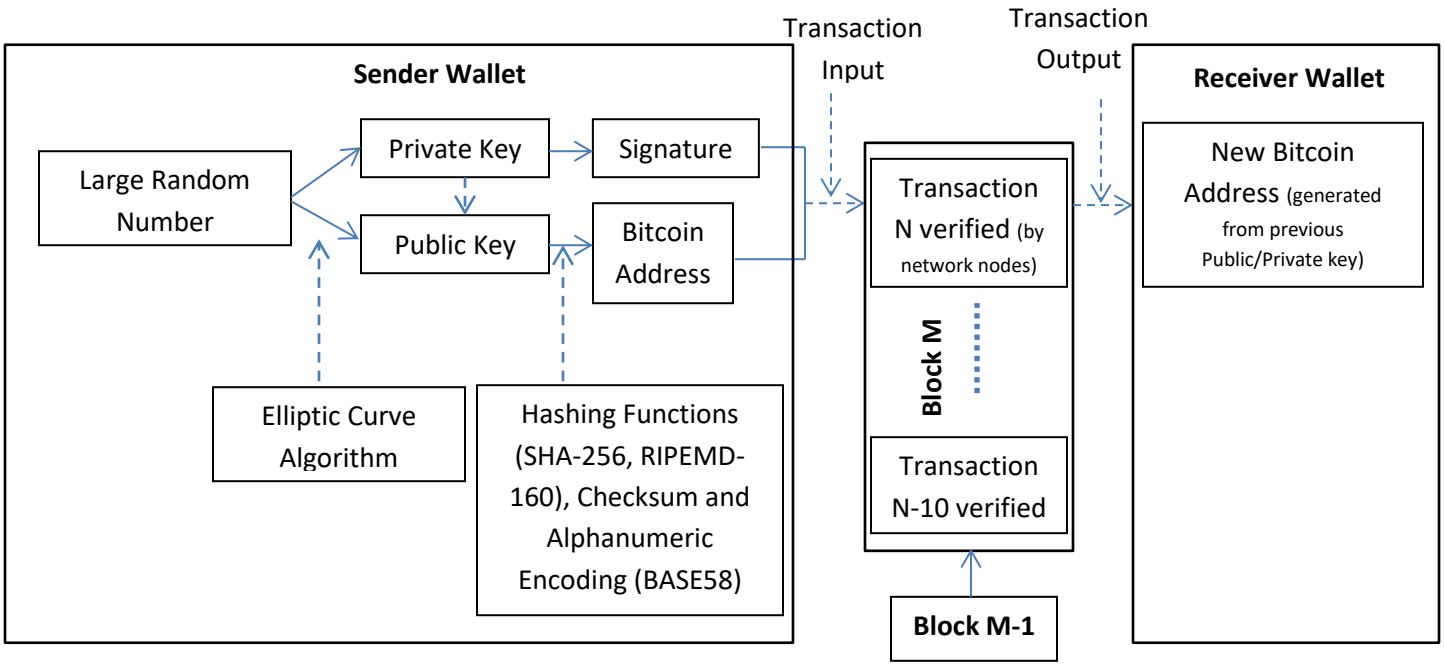
The current bitcoin protocol is adjusted so that on average, a block of transactions is processed every 10 minutes. This difficulty of the protocol is adjusted so that the rate of currencies generated is halved every 4 years and predictively will approach just under 21 million coins by the year 2140. Because of this negative fixed rate of coin issuance and its theoretical limit, bitcoin is considered "deflationary" and cannot be inflated above its issuance rate.

At a very high level view, a transaction is initiated by a random number that generates (by way of cryptographic hashing functions) a private and public key. The public key is further used to generate
A virtual wallet is necessary for receiving, storing, sending and managing bitcoins and is the primary user interface for the holder. It essentially holds the public addresses and private keys, keeps track of the balance and sings transactions. See Figure 1.

Bitcoin is a money protocol that is built on a decentralized network. Each node is independent and can join or leave the network at any time. While on the network, each node can talk to the other nodes using the Bitcoin protocol. With this protocol, it's able to script and validate the transactions or other types of digital contracts.

Bitcoin is essentially programmable money designed to run on a decentralized network.

Figure 1 – Basic Bitcoin Transaction



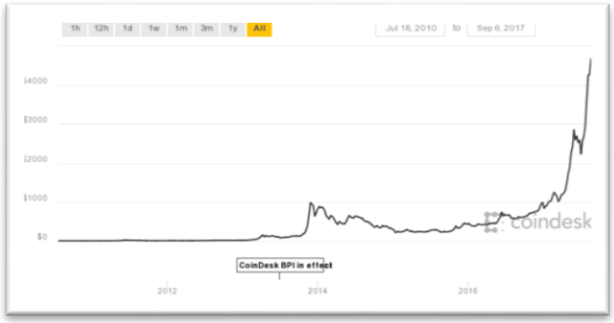
2. Product Evolution

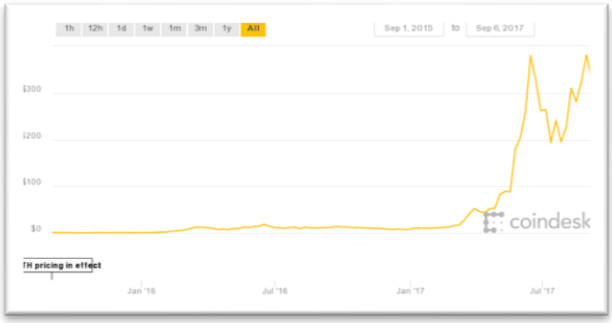
Since the mid 1990's, when internet flourished to become the next information revolution after the digital revolution of the PCs in the 70 and 80's, financial companies and markets begun to rely on electronic payments as a way to increase the speed, efficiency and reliability of money markets globally. From banks to credit cards and payment processors, electronic transfers, accounting and auditing of funds became the natural norm of a new integrated "real time" world economy.
However, the financial markets still lacked a critical component in order to be a real economic revolution as money was still in the form of a fiat currency and use centralized electronic money/centralized banking system. What was still lacking was an independent, decentralized and cyber safe virtual currency in which to transact.

The first decentralized cryptocurrency, bitcoin, was created in 2009 by pseudonymous developer Satoshi Nakamoto based on a paper published on 2008. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme. In October 2009 a Bitcoin exchange rate is established at $1USD = 1,309.03 BTC. Then in May 2010, the first real world transaction took place, with a developer purchasing two pizzas for 10,000 BTCs, and later that year Mt Gox , one of the first bitcoin exchanges opens doors and the market cap reaches $1 million. In February 2011, Bitcoin reaches parity with the US dollar. After the largest bubble burst of Bitcoin and the closure of Mt Gox due to the largest fraud on record for this currency, Bitcoin began an astronomical ascent, with thousands of companies across industries beginning to accept one way or another payment in the virtual currency, that has only been restrained with the news of governments calling for

scrutiny and regulation of the market. In the US, recent moves by the SEC, the Federal Reserve and the IRS have increased scrutiny and oversight but nonetheless coming short of restricting and imposing further controls. In 2016, Japanese government authorities recognized virtual currencies as a genuine and legal payment method. China on the other hand, after letting the altcurrency market lose for a few years, has started to impose grater controls, with a recent call for an immediate stop of Initial Coin Offerings (ICOs), a blockchain-based startup companies obtain their seed funding through the issuance of tokens usually sold in exchange for cryptocurrencies (mainly bitcoins and ethers).

In April 2011, Namecoin was created as an attempt at forming a decentralized DNS, which would make internet censorship very difficult. Soon after, in October 2011, Litecoin was released. It was the first successful cryptocurrency to use scrypt as its hash function instead of SHA-256. Another notable cryptocurrency, Peercoin was the first to use a proof-of-work/proof-of-stake hybrid. Many other cryptocurrencies have been created though few have been successful, as they have brought little in the way of technical innovation. On 6 August 2014, the UK announced its Treasury had been commissioned to do a study of cryptocurrencies, and what role, if any, they can play in the UK economy. The study was also to report on whether regulation should be considered

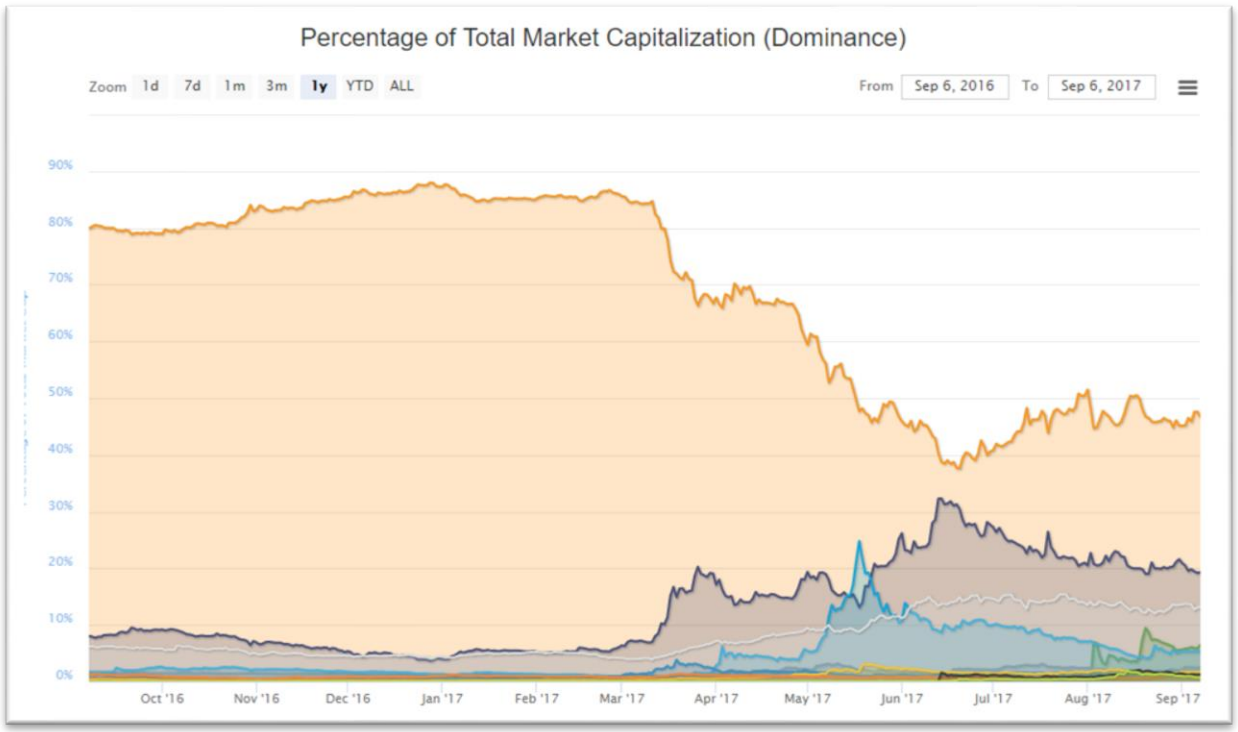




Source: Coindesk.com

3. Main Altcurrencies

Today, cryptocurrencies have a combined market cap value of $158 billion of which Bitcoin remains the largest one representing almost 50%.



Source: Coinmarketcap.com

Other main altcurrencies are:

Ethereum - Launched in 2015, Ethereum is a decentralized software platform that enables Smart Contracts (ie. contracts where there's no trusted third party) and Distributed Applications (aka DApps) to be built and run without any downtime, fraud, control or interference from a third party. Ethereum is not just a platform but also a programming language (aka Turing complete) running on a blockchain, helping developers to build and publish distributed applications. The potential applications of Ethereum are wide ranging.

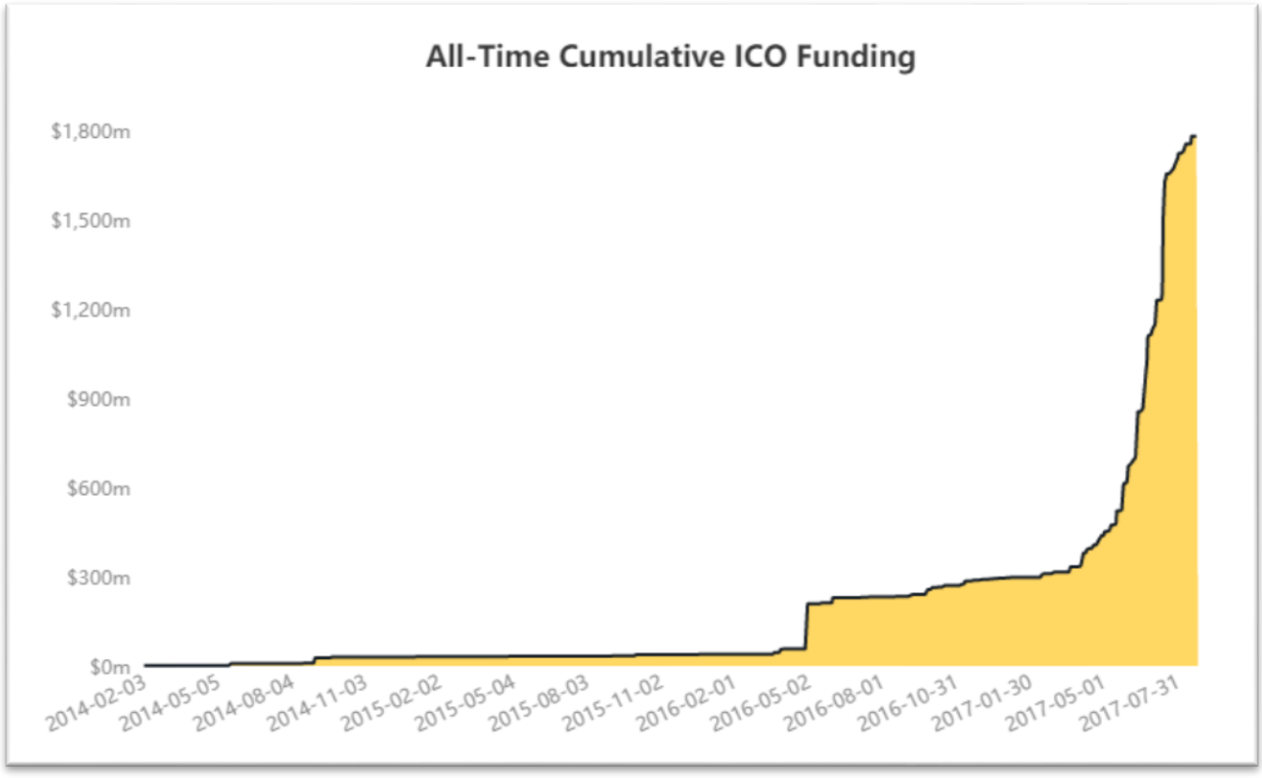
Bitcoin Cash – It is a fully decentralized peer-to-peer digital cash, with no central bank and requires no trusted third parties to operate. As a fork (ie. separation) of the Bitcoin blockchain ledger, with upgraded consensus rules that allow it to grow and scale by raising the block size limit to 8MB (from 1MB), it was born as part of a massive on-chain scaling approach by developers, miners and users who grew frustrated of skyrocketing fees, unreliability and long confirmation delays as a result of the Bitcoin network capacity hitting the 'invisible wall' originally set by its creator. The goal of this new currency it to achieve lower transaction fees and faster confirmations, so the network can lure back users, merchants, businesses, and investors.

Litecoin – Technically very similar to Bitcoin, but allows a greater number of transactions to be processed by the network in a given time, reducing potential bottlenecks, allowing it to have almost zero payment cost and facilitating payments approximately four times faster than Bitcoin. It became the first altcurrency to adopt a revised network verification protocol (Segregated Witness or SegWit) using an extended block for witness execution and virtually increase the block size thereby achieving faster confirmations as well as Lightning Network, a peer-to-peer system for making secured micropayments of digital currencies routed across payment channels with ultrafast payments and reduced blockchain load.

4. Applications

Although Bitcoin and its blockchain protocol were created primarily with an economic motive, its actual and potential applications are significantly broader. Besides serving as a reserve currency that cannot be manipulated by central banks, these currencies (especially Bitcoins) can be used to facilitate peer-to-peer transactions as well as any kind of transaction easily and safely, and soon it will be done swiftly.

In addition, the blockchain protocol and different verification methods and technologies around cryptographic hashing have given life to decentralized apps besides wallets for P2P payments, such as smart contracts that use the distributed ledger to keep track of states of the contracts, from insurance to financial derivatives clearing and settlements can be created. In theory, a true "leaderless" company, with given set of voting and governance rules, can also easily be designed to be funded and run. Recognizing these advantages, since 2016 startup companies (especially the ones working with blockchain Dapps) have begun issuing Initial Coin Offerings or ICOs, selling company tokens in exchange for altcurrencies (especially Ethers), as a way to finance their initial developments to run their networks.



Source: Coindesk.com

Leonardo Reos
President and Founder at Sigma Capital Advisors LLC

DISCLAIMER

This website and its blog is a publication of Sigma Capital Advisors LLC, a company incorporated in the state of Maryland. Information presented is believed to be factual and up-to-date, but we do not guarantee its accuracy and it should not be regarded as a complete analysis of the subjects discussed. All expressions of opinion reflect the judgment of the authors as of the date of publication and are subject to change. Information on this website and its blog do not involve the rendering of personalized investment advice. A professional advisor should be consulted before implementing any of the options presented. No content should not be construed as legal or tax advice. Always consult an attorney or tax professional regarding your specific legal or tax situation. Information on this website and blog is not an offer to buy or sell, or a solicitation of any offer to buy or sell the securities mentioned herein. Case studies are for illustrative purposes only and should not be construed as a testimonial. They do not represent the experience of any specific advisory client. Each investor situation is different, and goals may not always be achieved. It is unknown if the client approved or disapproved of the services rendered. None of the persons photographed is a current or former client of Sigma Capital Advisors LLC. These photos should not be construed as an endorsement or testimonial from them. Hyperlinks on this website are provided as a convenience. Sigma Capital Advisors LLC disclaims any responsibility for information, services, or products found on websites linked hereto. Additionally, Sigma Capital Advisors LLC is not liable for any direct or indirect technical or system issues or any consequences arising out of your access to or your use of third-party technologies, websites, information and programs made available through this website. When you access one of these websites, you are leaving our website and assume total responsibility and risk for your use of the websites you are linking to. Sigma Capital Advisors LLC is NOT registered as an investment advisor with the U.S. Securities Exchange Commission ("SEC") nor with any US state. Its owner and president is currently an Exempt Reporting Adviser ("ERA") in the state of Maryland that is not required to register as an adviser with the SEC or the state regulator, but must still pay fees and report public information via the IARD/FINRA system, and currently only transact in states where it is excluded or exempted from registration requirements. Different types of investments involve varying degrees of risk, and there can be no assurance that any specific investment will either be suitable or profitable for your portfolio. All investment strategies have the potential for profit or loss and past performance is no guarantee of future success. Historical performance results for investment indexes and/or categories, generally do not reflect the deduction of transaction and/or custodial charges or the deduction of an investment-management fee, the incurrence of which would have the effect of decreasing historical performance results. Economic factors, market conditions, and investment strategies will affect the performance of any portfolio and there are no assurances that it will match or outperform any particular benchmark.