

## Management of Cryptocurrency

**Name of the Author : Farhat Aziz Lone**

**Institution/Organization**

**/University Author : Chandigarh University Punjab (scholar)**

**Professional/Educational**

**Details : MBA (Finance)**

**Name of the co-author : Samina Jamaal**

**Institution/Organization : University of Kashmir Srinagar (scholar)**

**Professional/Educational**

**Details : MBA (Finance)**

**Management of Cryptocurrency**

**Table of content**

- Introduction
- History
- Working of cryptocurrency
- Transactions underlying Cryptocurrency
- Market Capitalization of Cryptocurrency
- Legal concerns of the Cryptocurrency
- Funding ICO
- Other forms of virtual currency
- Countries having operational cryptocurrency
- References

**KEY WORDS: CRYPTOCURRENCY, BITCOIN, BLOCKCHAIN.**

## 1. INTRODUCTION

Today **cryptocurrency** have become a global phenomenon known to most people. The revolution is already happening Institutional investors start to buy cryptocurrencies. Banks and governments realize that this invention has the potential to draw their control away. Cryptocurrencies is changing the world step by step. You can either stand beside and observe or you can become part of history .A **cryptocurrency** is a virtual currency and digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Technology advancements all over the globe are driving disrupting changes in the traditional way of doing things including the way goods and services are acquired and paid for. The rise of cross-border and e-commerce platforms for shopping has led to a demand for alternative means of making payments in digital world is virtual currency. Virtual currency is a type of digital money that is used to purchase real-world goods and services. The most popular form of virtual currency is known as Bitcoin. Bitcoin runs on a decentralized peer-to-peer currency network. It bypasses the regulatory operations of central banks and central clearing houses which exist to monitor, verify, and approve transactions in legal tender. The value of a Bitcoin in dollars has been exchanged from as low as \$13 sometime in 2012 to as high as \$1250 in 2013. As of 2016, the value of Bitcoin is determined to fall between the range of \$350 and \$660. Virtual currency can be converted for cash through online exchanges. Exchanges such as Coinbase and Bitstamp enable users to exchange their Bitcoin for their local currency. The Bitcoin holder makes a sell order like s/he would if making a trade with a securities broker. The sell order includes the number of Bitcoin and price per coin. The user's account is credited in the local currency when his/her order is matched to a corresponding buy order. Convertible virtual currencies can also be exchanged for real currency using Bitcoin ATMs which take only seconds to complete the transaction .A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency is it uses decentralized control as opposed to centralized electronic money and central banking systems. It is not issued by any central authority, this way it is immune from any government interference or manipulation. Cryptocurrencies make it easier to transfer funds between two parties in a transaction; these transfers are facilitated through the use of public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks and financial institutions for wire transfers .The decentralized control is related to the use of bitcoin's blockchain, which is transaction database in the role of a distributed ledger. Within cryptocurrency systems the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners which are members of the general public using their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme. Miners have a financial incentive to maintain the security of a cryptocurrency ledger. The first cryptocurrency was Bitcoin, which was launched in 2009 by an individual Satoshi Nakamoto 'A Peer-to-Peer Electronic Cash System'. Since then, numerous other cryptocurrencies have been created. These are frequently called **altcoins**, as a blend of **alternative coin**. As of September 2015, there were over 14.6 million bitcoins in circulation with a total market value of \$3.4 billion. Bitcoin's success has spawned a number of competing cryptocurrencies,

such as **Litecoin, Namecoin and PPCoin**. However, because cryptocurrencies are virtual and do not have a central repository, a digital cryptocurrency balance can be wiped out by a computer crash if a backup copy of the holdings does not exist. Since prices are based on supply and demand, the rate at which a cryptocurrency can be exchanged for another currency can fluctuate widely. The anonymous nature of cryptocurrency transactions makes them well-suited for a host of nefarious activities, such as money laundering and tax evasion.

Cryptocurrencies are not immune to the threat of hacking. In Bitcoin's short history, the company has been subject to over 40 thefts, including a few that exceeded \$1 million in value. Still, many observers look at cryptocurrencies as hope that a currency can exist that preserves value, facilitates exchange, is more transportable than hard metals, and is outside the influence of central banks and governments. Jordan Kelley, founder of Robocoin, launched the first Bitcoin ATM in United States in 2014. The kiosk installed in Austin, Texas is similar to bank ATMs but has scanners to read government-issued identification such as a driver's license or a passport to confirm users' identities. By 2017 1574 Bitcoin ATMs were installed around the world with an average fee of 9.05%. An average of 3 Bitcoin ATMs was being installed per day in September 2017.

## II.HISTORY

In 1998, Wei Dai published a description of "b-money", an anonymous, distributed electronic cash system. Shortly thereafter, Nick Szabo created "bit gold". Like Bitcoin and other cryptocurrencies that would follow it, bit gold was an electronic currency system which required users to complete a proof of work function with solutions being cryptographically put together and published. A currency system based on a reusable proof of work was later created by Hal Finney who followed the work of Dai and Szabo. The first decentralized cryptocurrency, bitcoin, was created in 2009 by pseudonymous developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme. 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. IOTA was the first cryptocurrency not based on a blockchain, and instead uses the Tangle. Built on a custom blockchain, many other cryptocurrencies have been created though few have been successful, as they have brought little in the way of technical innovation. In 2014, the UK made a study on cryptocurrencies. Cryptocurrencies by simple definition is limited entries in a database no one can change without fulfilling specific conditions take the money on your bank account: What is it more than entries in a database that can only be changed under specific conditions. Money is all about a verified entry in some kind of database of accounts, balances, and transactions.

## III.WORKING OF CRYPTOCURRENCY

### Bitcoin Exchange

A Bitcoin exchange is a digital marketplace where traders can buy and sell bitcoins using different fiat currencies or altcoins. A Bitcoin currency exchange is an online platform that acts as an intermediary between

buyers and sellers of the cryptocurrency. The currency ticker used for Bitcoin is either BTC or XBT. Bitcoin exchange platforms match buyers with sellers. Like a traditional stock exchange, traders can opt to buy and sell Bitcoin by inputting either a market order or a limit order. When a market order is selected, the trader is authorizing the exchange to trade his coins for the best available price in the online marketplace. With a limit order set, the trader directs the exchange to trade coins for a price below the current ask or above the current bid, depending on whether s/he is buying or selling. Bitcoin Unlimited a proposed upgrade to Bitcoin Core that allows larger block sizes. Bitcoin Unlimited is designed to improve transaction speed through scale. The problem that a digital currency or token can be used in more than one transaction is not found in physical currencies, as a physical bill or coin can, by its nature, only exist in one place at a single time. Since a digital currency does not exist in the physical space, using it in a transaction does not remove it from someone's possession. The software standard for Bitcoin developed by Nakamoto is referred to as Bitcoin or Bitcoin Core. Since its launch, a number of improvements to the software have been proposed. These proposals often focus on increasing the number of transactions that the system can handle, either by speeding up the process or by increasing the size of Bitcoin blocks. Blocks are files where Bitcoin network data is permanently recorded. A block records recent Bitcoin transactions, and serves a similar purpose as a ledger page or record book. Each time a block is completed it gives way to the next block in the blockchain. Blocks in Bitcoin Core are limited to one megabyte. Bitcoin Unlimited proposed that the size of blocks should be increased, and that miners which are individuals and companies that provide the computing power required to maintain records of Bitcoin transactions will step up to increase capacity. Because Bitcoin is not controlled by a single entity, decisions concerning upgrades are done through consensus. One of the primary reasons for this approach is that any organization that pushes forward with a change that other groups have not agreed to can result in Bitcoin "forking", which means that the network that runs bitcoin splits between different standards. A consensus-driven approach can, however, make it harder to tackle issues that bitcoin adoption faces. Concern over forking is one of the reasons why Bitcoin Unlimited is not the new standard. Another concern voiced over Bitcoin Unlimited is that allowing bigger blocks could result in only miners with large processing power being profitable, while smaller miners with more limited resources will be pushed out. The concentration of capacity generation in the hands of fewer miners could increase costs. Proponents of Bitcoin Unlimited believe that moving away from the block size limit will democratize the system, as miners and node owners are free to choose how large of a block size to accept. To realize digital cash you need a payment network with accounts, balances, and transaction this is done by a central server who keeps record about the balances. A change in ownership of an asset, or a movement of funds and/or assets from one account to another. When an account holder moves funds from one account to another, transfer has occurred. The transfer does not have to be within the same bank, it can be an interbank transfer from one account held at Bank A to another held at Bank B. Within the banking industry, funds can also be transferred cross-border through wire transfers from a domestic account to a foreign account, and vice versa. The receiving accounts could be held by the same account holder or could be owned by a different person or company. Funds are normally transferred for purposes of **Financial planning**, investment, goods or services, gift, to save money, etc.

- **Brokerage:** Investors normally transfer funds and assets from within or outside their brokerage accounts. Most assets like company stock, bonds, certificates of deposit (CDs), mutual funds, etc. can be transferred in-kind from one investment account to another.
- **Cryptocurrency:** In the crypto economy, funds and cryptocurrencies are transferred frequently between users to public addresses where the funds can be accessed with a private key unique to each user. When goods and services are traded, the buyer would transfer; say Bitcoin, from his holdings to the seller's digital address
- **Asset Title:** Titles on assets like cars, land, and homes can be transferred when sold or gifted to an individual or corporation.
- **Loan Transfer:** A homeowner with an assumable loan can transfer the mortgage to someone else, say the buyer, if s/he qualifies for the loan. This could be a win-win solution for both parties involved in the transaction.
- **Transactions underlying cryptocurrency**

The transaction is known almost immediately by the whole network. But only after a specific amount of time it gets confirmed. Confirmation is a critical concept in cryptocurrencies. You could say that cryptocurrencies are all about confirmation. As long as a transaction is unconfirmed, it is pending and can be forged. When a transaction is confirmed, it is set in stone. It is no longer forgeable, it can't be reversed, it is part of an immutable record of historical transactions: of the so-called blockchain. Only miners can confirm transactions. This is their job in a cryptocurrency-network. They take transactions, stamp them as legit and spread them in the network. After a transaction is confirmed by a miner, every node has to add it to its database. It has become part of the blockchain. For this job, the miners get rewarded with a token of the cryptocurrency, for example with Bitcoin. The databases of cryptocurrencies like Bitcoin consist of a network of peers. Every peer has a record of the complete history of all transactions and balance of every account. Bitcoin, as a decentralized network of peers which keep a consensus about accounts and balances, is more a currency than the numbers you see in your bank account. A database which can be changed by people you don't see and by rules you don't know.

Basically, cryptocurrencies are entries about token in decentralized consensus-databases. They are called **cryptocurrency** because the consensus-keeping process is secured by strong cryptography. The properties of cryptocurrencies we need to separate between transactional and monetary properties.

- **Transactional properties:**

- **Irreversible:** After confirmation, a transaction can't be reversed.
- **Pseudonymous:** Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters.
- **Fast and global:** Transaction is propagated nearly instantly in the network and is confirmed in a couple of minutes. Since they happen in a global network of computers they are completely indifferent of your physical location.
- **Secure:** Crypto currency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers make it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.

□ **Permission less:** You don't have to ask anybody to use cryptocurrency. It's just a software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.

- **Monetary properties:**

□ **Controlled supply:** Most cryptocurrencies limit the supply of the tokens. In Bitcoin, the supply decreases in time and will reach its final number somewhere in around 2140. All cryptocurrencies control the supply of the token by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. There is no surprise.

□ **No debt but bearer:** The Fiat-money on your bank account is created by debt, and the numbers, you see on your ledger represent nothing but debts. It's a system of IOU. Cryptocurrencies don't represent debts. They just represent themselves. They are money as hard as coins of gold.

- **Market Capitalization of Cryptocurrency**

The Crypto Currencies Index CCI30 index is composed of the 30 crypto currencies with the biggest market capitalization. It was created by a team of mathematicians, quantitative analysts and traders, led by Professor **Igor Rivin** and **Carlo Scvola**, economist. The components of the index are set at a fixed number of 30, weighted based on the square root of their smoothed market capitalization. The composition of the index is revised on a quarterly basis, using an exponentially weighted moving average of the market capitalization.

The CCI30 starts in January 2015 with a value of 100. This index is freely available to the public, and can be replicated by funds that follow a passive investment strategy. Cryptocurrencies are used primarily outside existing banking and governmental institutions, and exchanged over the Internet. While these alternative, decentralized modes of exchange are in the early stages of development, they have the unique potential to challenge existing systems of currency and payments. As of December 2017 total market capitalization of cryptocurrencies is bigger than 600 billion USD and record high daily volume is larger than 50 billion USD. As of January 2018, there were over 1384 and growing digital currencies in existence

- **Indices**

In order to follow the development of the market of cryptocurrencies, indices keep track of notable cryptocurrencies and their cumulative market value.

- **Crypto index CRIX**

The cryptocurrency index CRIX is a conceptual measurement jointly developed by statisticians at Humboldt University of Berlin, Singapore Management University and the enterprise Coin Gecko and was launched in 2016. The market of crypto currencies is fast and wild. Nearly every day new cryptocurrencies emerge, old die, early adopters get wealthy and investors lose money. Every cryptocurrency comes with a promise, mostly a big story to turn the world around. Few survive the first months, and most are pumped and dumped by speculators and live on as zombie coins until the last bag holder loses hope ever to see a return on his investment.

- **Legal concerns of the cryptocurrency**

The legal status of cryptocurrency varies substantially from country to country and is still undefined or changing. While some countries have explicitly allowed their use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. China

Central Bank banned the handling of bitcoins by financial institutions in China during an extremely fast adoption period in early 2014. In Russia, though crypto currencies are legal, it is illegal to actually purchase goods with any currency other than the Russian ruble. The United States Internal Revenue Service (IRS) ruled that Bitcoin will be treated as property for tax purposes as opposed to currency. This means bitcoin will be subject to capital gains tax. One benefit of this ruling is that it clarifies the legality of bitcoin. The Cryptocurrency Alliance Super PAC One of the many groups formed to protect consumer interests in cryptocurrencies. Legal issues not dealing with governments have also arisen for cryptocurrencies. Coinye, for example, is an altcoin that used rapper Kanye West as its logo without permission. Upon hearing of the release of Coinye, originally called Coinye West, attorneys for Kanye West sent a cease and desist letter to the email operator of Coinye, David P. McEnery Jr. The legal concern of an unregulated global economy. As the popularity of and demand for online currencies has increased since the inception of bitcoin in 2009, so have concerns that such an unregulated person to person global economy that cryptocurrencies offer may become a threat to society. Concerns abound that altcoins may become tools for anonymous web criminals. Transactions that occur through the use and exchange of these altcoins are independent from formal banking systems, possible tax evasion for individuals. Systems of anonymity that most cryptocurrencies offer can also serve as a simpler means to launder money, Loss, theft, and fraud, Darknet markets. Cryptocurrency is also used in controversial settings in the form of online black markets such as Silk Road. Darknet markets present growing challenges in regard to legality. Bitcoins and other forms of cryptocurrency used in dark markets are not clearly or legally classified in almost all parts of the world. Since most darknet markets run through Tor, they can be found with relative ease on public domains.

- **Funding's – ICOs**

□ An initial coin offering (ICO) is an unregulated means by which funds are raised for a new cryptocurrency venture. An ICO is used by startups to bypass rigorous and regulated capital raising processes required by venture capitalists or banks. In an ICO campaign, a percentage of the cryptocurrency is sold to early backers of the project in exchange for legal tender or other cryptocurrencies, often Bitcoin or Ethereum.

- **Proof of work and proof of stake and other schemes**

- **Timestamping**

Cryptocurrencies use various timestamping schemes to avoid the need for a trusted third party to timestamp transactions added to the blockchain ledger.

- **Proof-of-work schemes**

The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256, which was introduced by Bitcoin, and scrypt, which is used by currencies such as Litecoin. Some other hashing algorithms that are used for proof-of-work include CryptoNight, Blake, SHA-3, and X11. Modifications of the proof-of-work algorithm have been created to address the problem of scaling, such as the way the IOTA ledger works. IOTA uses a simplified Proof-of-work algorithm making use of directed acyclic graph. A new transaction becomes part of the ledger after its sender does a small amount of proof-of-work. Each network participant is therefore also a miner, however without any economic incentive other than enabling their own transactions.

- **Proof of Stake (PoS)**

Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to the coins held. This means that the more Bitcoin or altcoin owned by a miner, the more mining power. The first cryptocurrency to adopt the PoS method was Peercoin. Nxt, Blackcoin, and ShadowCoin soon followed suit. The proof of stake was created as an alternative to the proof of work (PoW), to tackle inherent issues in the latter. When a transaction is initiated, the transaction data is fitted into a block with a maximum capacity of 1 megabyte, and then duplicated across multiple computers or nodes on the network. The nodes are the administrative body of the blockchain and verify the legitimacy of the transactions in each block. To carry out the verification step, the nodes or miners would need to solve a computational puzzle, known as the proof of work problem. The first miner to decrypt each block transaction problem gets rewarded with coin. Once a block of transactions has been verified, it is added to the blockchain, a public transparent ledger. Mining requires a great deal of computing power to run different cryptographic calculations to unlock the computational challenges. The computing power translates into a high amount of electricity and power needed for the proof of work. In 2015, it was estimated that one Bitcoin transaction required the amount of electricity needed to power up 1.57 American households per day. To foot the electricity bill, miners would usually sell their awarded coins for fiat money, which would lead to a downward movement in the price of the cryptocurrency. The proof of stake (PoS) seeks to address this issue by attributing mining power to the proportion of coins held by a miner. This way, instead of utilizing energy to answer Pow puzzles, a PoS miner is limited to mining a percentage of transactions that is reflective of his or her ownership stake. For instance, a miner who owns 3% of the Bitcoin available can theoretically mine only 3% of the blocks. Bitcoin uses a PoW system and as such is susceptible to a potential Tragedy of Commons. The Tragedy of Commons refers to a future point in time when there will be fewer Bitcoin miners available due to little to no block reward from mining. The only fees that will be earned will come from transaction fees which will also diminish over time as users opt to pay lower fees for their transactions. With fewer miners than required mining for coins, the network becomes more vulnerable to a 51% attack. A 51% attack is when a miner or mining pool controls 51% of the computational power of the network and creates fraudulent blocks of transactions for him, while invalidating the transactions of others in the network. With PoS, the attacker would need to obtain 51% of the cryptocurrency to carry out a 51% attack. The proof of stake avoids this 'tragedy' by making it disadvantageous for a miner with a 51% stake in a cryptocurrency to attack the network. Although it would be difficult and expensive to accumulate 51% of a reputable digital coin, a miner with 51% stake in the coin would not have it in his best interest to attack a network which he holds a majority share. If the value of the cryptocurrency falls, this means that the value of his holdings would also fall, and so the majority stake owner would be more incentivized to maintain a secure network. In addition to Bitcoin, Litecoin (LTC) also uses the PoW method. Nxt (NXT) is an example of a cryptocoin that uses the PoS method. Some coins like Peercoin (PPC) use a mixed system where both methods are incorporated. As of May 2017, Ethereum (ETH) is in the process of completely switching from a PoW to a PoS system.

- **Other forms of virtual currency**
- **Litecoin**

Launched in the year 2011, Litecoin is an alternative cryptocurrency based on the model of Bitcoin. Charlie Lee, a MIT graduate and former Google engineer, is Litecoin's creator. Litecoin is based on an open source global payment network that is not controlled by any central authority. Litecoin differs from Bitcoin in aspects like faster block generation rate and use of scrypt as a proof of work scheme. Litecoins were launched with the aim of being the "silver" to Bitcoin's "gold," and have gained much popularity since the time of inception. Litecoin is designed to produce more coins (Four times that of Bitcoin) and at a faster rate (1/4th of the time of Bitcoin). Overall, Litecoin is seen as second to Bitcoins in value, but Litecoins are more easily obtainable and transactional.

- **Altcoin**

Altcoins are the alternative cryptocurrency of Bitcoin. Many altcoins modify the limitations that Bitcoin has and come up with newer versions with competitive advantages. There is a great variety of altcoins."Altcoin" is a combination of two words: "alt" and "coin"; alt is short for alternative and coin signifies currency. Many of the altcoins are built up on the basic framework provided by Bitcoins. Even with many close competitors, Bitcoin is still leading the virtual currency pack. Newer and more innovative versions are getting launched that offer modifications in areas like transaction speed, privacy, proof-of-stake, DNS resolution and more. A few of them have gained popularity; the rest are lesser-known. Examples of altcoin include Litecoin, Dogecoin, Peercoin, Feathercoin, Zetacoin, Novacoin, etc. Litecoin is seen as the closest competitor to Bitcoin.

- **Bitcoin XT**

A fork from Bitcoin Core that proposed increasing the size of blocks from one megabyte to eight megabytes. Bitcoin XT gained first attention in 2015.

- **Ethereum**

The brainchild of young crypto-genius Vitalik Buterin has ascended to the second place in the hierarchy of cryptocurrencies. Other than Bitcoin its blockchain does not only validate a set of accounts and balances but of so-called states. This means that Ethereum can not only process transactions but complex contracts and programs. This flexibility makes Ethereum the perfect instrument for blockchain -application. But it comes at a cost. After the Hack of the DAO – an Ethereum based smart contract – the developers decided to do a hard fork without consensus, which resulted in the emerge of Ethereum Classic. Besides this, there are several clones of Ethereum, and Ethereum itself is a host of several Tokens like Digix DAO and Augur. This makes Ethereum more a family of cryptocurrencies than a single currency.

- **Ripple**

Maybe the less popular or most hated project in the cryptocurrency community is Ripple. While Ripple has a native cryptocurrency XRP it is more about a network to process IOUs than the cryptocurrency itself. XRP, the currency, doesn't serve as a medium to store and exchange value, but more as a token to protect the network against spam. Ripple Labs created every XRP-token, the company running the Ripple network, and is distributed by them on will. For this reason, Ripple is often called pre-mined in the community and disassessed as no real cryptocurrency, and XRP is not considered as a good store of value .Banks, however, seem to like Ripple. At least they adopt the system with an increasing pace.

- **Monero**

Monero is the most prominent example of the cryptonite algorithm. This algorithm was invented to add the privacy features Bitcoin is missing. If you use Bitcoin, every transaction is documented in the blockchain and the trail of transactions can be followed. With the introduction of a concept called ring-signatures, the cryptonite algorithm was able to cut through that trail. The first implementation of cryptonite, Bytecoin, was heavily premined and thus rejected by the community. Monero was the first non-premined clone of bytecoin and raised a lot of awareness. There are several other incarnations of cryptonote with their own little improvements, but none of it did ever achieve the same popularity as Monero. Monero popularity peaked in summer 2016 when some darknet markets decided to accept it as a currency. This resulted in a steady increase in the price, while the actual usage of Monero seems to remain disappointingly small. Besides those, there are hundreds of cryptocurrencies of several families. Most of them are nothing more than attempts to reach investors and quickly make money, but a lot of them promise playgrounds to test innovations in cryptocurrency-technology.

#### **IV. COUNTRIES HAVING OPERATIONAL CRYPTO CURRENCY**

- BAHRAIN
- QATAR
- THE UNITED ARAB EMIRATES
- UNITED KINGDOM
- SOUTH AFRICA
- SINGAPORE

#### **REFERENCES**

- Wikipedia
- Handbook of digital currency: bitcoin, innovation, financial instruments, and big data Lee
- KuoChuen, David,. Amsterdam.
- www.investopedia.com
- Nick Szabo "Bitcoin"
- Satoshi Nakamoto "Bitcoin P2P e-cash paper "
- Economist Staff "Blockchains: The great chain of being sure about things". The Economist
- Wallace, Benjamin "The Rise and Fall of Bitcoin".
- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System