Version 1.0

Seizing Opportunities In The Blockchain & Digital Currency REVOLUTION

A Handbook for Enthusiasts

Chimezie Chuta

Title Page

Seizing Opportunities in the
Blockchain & Digital Currency Revolution

A Handbook for Enthusiasts

Version 1.0

By Chimezie Chuta

ISBN: 978-1500655945

July 2017

Published by
Web Print Express Services Inc.

34 Shipeolu Street, Palmgrove, Lagos, Nigeria

Tel: +2348165430776

Email: info@webprintex.com

Website: http://webprintex.com

Introduction

Unless one has been living under a rock, or perhaps returning from a long space trip, chances are that you have heard about the Blockchain Technology or its first fruit Digital Currency known as Bitcoin. Blockchain and cryptocurrency are the hottest topics on most people's lips these days. But whether or not the subject is fully understood, is altogether, a different kettle of fish. However, pockets of information is scattered all over the internet. Most of such materials are highly technical and far beyond the understanding of an average educated person, let alone that of unschooled persons. Yes, some level of education is relevant in other to understand technology, but if technology is not broken down to the level of understanding of the majority, massive adoption will remain elusive.

So far, the only set of people who can truly understand the blockchain technology are techie people. The reason is not far-fetched: they have been familiar with its technology ancestors and forerunners hence they easily navigate the waters with classical sophistication. But what about the billions of people around the word that are not that fortunate to be listed among tech savvies? People that don't understand "Hashes" "Protocols," “algorithm” etc?

This book is for you if you find yourself in that group.

Explaining The Blockchain Technology and stripping it of its technicalities is like serving a dish to an ulcer patient. No spicing, all the bells and whistles are taken out.

But it is still edible.

This book promises to be a non-technical guide, albeit a very tasking undertaking!

Because this handbook is intended for the beginner blockchain/ crypto enthusiast reader, it may suffer from the same errors inherent when a complex topic is (over?) simplified.

It's my hope that this promise of simplicity will be kept all through the reading.

If you get lost at any point, please forgive me.

There are land mines on every part of the road down the rabbit hole. Without the warnings inherent in this book, you could lose a lot of money at every juncture. I know because I was not that fortunate to find such useful guides early enough. So, I lost a lot of money. Therefore I have put this book together so you will not have the same ugly and painful experience I had.

One of my gifting is a passion for understanding difficult things at a fundamental level and the ability of sharing them as clearly as possible to anyone around me. This is what I have set out to do in this book.

Remember, the book is only a guide. As a guide, it's not exhaustive. You will still have to dig further on your own.

Talking about cryptocurrency and blockchain development is like trying to take a picture of a running cheetah. The pace is moving at breakneck speed, and any attempt to pin it or pen it down results in a blurry images. Regardless, I still believe it's important that we make concerted efforts efforts to educate as many people as possible on blockchain and cryptocurrency topics.

Blockchain and cryptocurrencies, combined with the power of the internet, gives individuals the tools to achieve financial independence. I will show you the various ways to make money in this rapid growing industry and how to take advantage of this opportunity. For instance, bitcoin was born out of the ashes of the 2008 global economic meltdown, as an alternative financial network that can bypass the banking system. During its 9 years of existence, it has proven to be one of the most profitable investments and store

of value. $100 worth of bitcoin in 2010 had a value of $10.8 million at the end of 2016. Bitcoin is the digital gold of the information age.

You will learn in this book, how to glean these opportunities and create trans-generational wealth for yourself.

Sadly, it is rare to find cryptocurrency topics discussed in schools or in academic circles. Given the barriers to understanding cryptocurrency and the large amount of misinformation/ propaganda, it is important that we take the bull by the horn and explain both the advantages and disadvantages of cryptocurrencies. Unfortunately, cryptocurrency is like a black box to vast majority of the people. What we need is to open the box and peer inside, in other to fully realize the potential hitherto locked inside.

If you feel that I've made any overreaching assumptions in this walk-through, please fire me a mail at chimeziechuta @gmail.com! I'd love to talk more and we can learn more whenever opportunity presents itself.

We need everyone's input to figure out the right path towards a healthy and sustainable cryptoeconomic future.

Note: The terms bitcoin, Digital currency, virtual currencies and crypto-currencies are sometimes used interchangeably in this book, even though I have tried to explain their differences in one of the chapters for clarity sake.

Chimezie Chuta,
Lagos, Nigeria
July 2017.

The Blockchain Technology

Definitions

A blockchain is an append-only, decentralized, distributed database.

A blockchain is a type of distributed ledger, comprised of unchangeable or immutable, digitally recorded data in packages called blocks.

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

The Blockchain is Transparent, incorruptible and time-stamped.

The blockchain network lives in a state of consensus, one that automatically checks in with itself every ten minutes. A kind of self-auditing ecosystem of a digital value, the network reconciles every transaction that happens in ten-minute intervals. Each group of these transactions is referred to as a "block". Two important properties result from this:

1. Transparency: Data is embedded within the network as a whole, by definition it is public.
2. It cannot be corrupted: Altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network. At least a 51% computing power of the entire network will be a starting point!

Blockchain technology is like the internet in that it has a built-in robustness. By storing blocks of information that are identical across its network, the blockchain cannot:

1. Be controlled by any single entity.
2. Has no single point of failure.

These digitally recorded "blocks" of data is stored in a linear chain. Each block in the chain contains data (e.g. bitcoin transaction), and is cryptographically hashed. The blocks of hashed data draw upon the previous-block (which came before it) in the chain, ensuring all data in the overall "blockchain" has not been tampered with and remains unchanged.

A network of computing "nodes" make up the blockchain.

Here is a simpler way to explain the blockchain.

A blockchain is a large digital record made out of a chain of digital data blocks. It's shared by 10,000 to 20,000 computers around the world, so there's no single master copy of it. It exists as identical copies on all those computers. Since nobody owns the blockchain—such as a government that could change hands or a private business that could fail—it's unusually safe from tampering, accidental loss or mishap.

The blockchain cannot be changed. It can only be added to. This ensures that all of the information it contain cannot be successfully altered.

All of this is accomplished only after they receive the requisite cryptographic and mathematical proof baked into the new block. (This is what puts the "crypto" in "cryptocurrency".) The process occurs automatically, requiring no human interaction or control, and typically takes just a few minutes.

The first blockchain ledger ever created was for bitcoin, and it set the pattern for many others — which represents the most innovative and potentially influential aspect of the technology. Participants interact with one another using pseudonyms, and their real identities are encrypted. The ledger uses public-key encryption, which is virtually impossible to break, because a message can be unlocked only when a public and a private element (the latter held only by the recipient) are linked.

The Pain

What problem does The Blockchain Technology solve?

The main problem that blockchain solves results from the fact that computer databases simply cannot talk to each other without a layer of expensive fault-prone human administration or bureaucratic central authority controlling every node. Blockchain technology, on the other hand, is a single, decentralized database managed by software and shared by multiple users, without any third party authority. This makes processing transactions less costly and less error-prone. This software enables process efficiency because new links can form as needed, and improves organizational efficiency because no management gatekeepers are needed.

By this process, single point of failure is completely eliminated. If one node goes offline, thousands remain online to ensure unbroken network. This had been a major problem for centralized databases.

The central problem in electronic cash is double spend. Because pure electronic money is just data, nothing stops a currency holder from trying to spend it twice. Blockchain solves the “Double Spend” problem without a digital reserve fund or similar form of umpire.

Blockchain monitors and verifies Digital Currency transactions by calling upon a decentralized network of volunteer-run nodes to, in effect, vote on the order in which transactions occur. The network's algorithm ensures that each transaction is unique.

The applicability of blockchains may include everywhere that many people may want to interact with a computer database. It is easy to imagine a tremendous breadth and depth of potential applications and markets.

Centralization

The traditional way to enable databases to communicate with each other is to consolidate and combine them into a single database, hoping that enough commonality would exist to patch them together. This approach is typical of mergers and acquisitions of corporations where two somewhat similar entities combine their data under a central authority. Efficiencies are gained in scale and elimination of redundancy. Unfortunately, centralization can also lead to inefficiencies such as top-heavy hierarchy, monopoly, obfuscation, stagnation and vulnerability to external shocks. Failures would often trigger blanket legislation and government regulations. Meanwhile, the original problem remains; how do these new mega databases communicate with other mega databases?

Decentralization

The other way to eliminate intermediaries and enable data to be shared between organizations is for everyone to share the same database. Multiple writers can retrieve and populate data simultaneously with no controls, consensus or centralized authority. Natural organic links would form, and operations would become faster, cheaper and easier to perform and maintain. The network effect can take hold where the value of the network would grow exponentially. Unfortunately, there would be no way to stop a person from cheating another person, or going back to change the conditions of a contract, or giving himself a raise, or double spending a unit of account, etc. For decentralized databases, these are precisely the problems that blockchain solves.

Before bitcoin, if a person sent a contract over email, each party would hold an identical copy that could be easily manipulated. After bitcoin, a person can send a contract electronically, and the receiving party would hold the only valid copy. While this may sound trivial at first, it is extraordinarily difficult for a computer to do. But it would allow computers to perform some of the functions that administrators routinely perform today at nearly every interaction with a computer.

Not unlike what happened with mechanization in the last century, once achieved, the software-managed architecture will be faster, more reliable and cheaper while the marginal cost of adding additional capacity approaches zero. Centralized databases scale at the speed of bureaucracy. Blockchain may scale up to handle large and complex transactions or scale down to accommodate billions of micro-transaction with little difference in operations cost. Also, like what happened with mechanization, society will certainly reorganize around these new forms of value creation and exchange.

Another pain point that the Blockchain Technology seeks to solve is document verification and identity. Databases become primary targets for hackers because of the centralized information that resides within them such as certificates, identities, property documents, title deeds etc. If the encryption of that database is cracked, the hacker can potentially steal all of the information that is being stored. Blockchain technology offers a unique solution to this problem by decentralizing all of this data. The data therefore wouldn't exist on one single server, but instead on a distributed public ledger being maintained by hundreds of thousands of computers all over the world. As a result, mass data hacks would be next to impossible to pull off since not one entity is in total control of all of the information.

Finally a Trust or God Protocol

In 1998, Nick Szabo published a short paper entitled “The God Protocol.” He wrote about the formation of a be-all end-all technology protocol, one that chose God the trusted 3rd party in the middle of all transactions. Nick's idea was powerful: doing business on the Internet needs a leap of faith. By the way, I heard Nick Szabo is a time traveler from the year 2214. It's a joke!

Nick was the founder of the early digital currency eCash of 1998.

He said

"God being the ultimate in confessional discretion, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output."

Ten years later in 2008, Satoshi Nakamoto (an unknown, faceless person, group or pseudonym) came up with this new protocol for a peer-to-peer electronic money system using a cryptocurrency he called bitcoin. This protocol established the rules that ensured the integrity of the information exchanged among millions of devices without passing through a trusted 3rd party. Consequently, that act set off a spark that terrified, excited or otherwise captured people's imagination in the computing world and spread everywhere like wild fire.

Today, people everywhere are trying to know the implications of a protocol that allows humans to create trust via clever code. This protocol is the foundation of the blockchain: the technology that enables trusted transactions between two or more people, validated by mass cooperation and powered by shared self-interests, rather than by big corporations that are driven by greed and profit.

With blockchain, the internet of information has transformed to the internet of value. .

Open Source vs Closed Source

Why is this important?

Clear understanding of computer software models is very important in understanding and following up on our on-going discussion on the blockchain technology.

In Software terms, open source refers to a software which has it's source code freely available on the Internet for public download. In comparison, the

source code for proprietary commercial software is usually a closely guarded secret of the company.

Open source software is distributed under different types of licenses such as LGPL, GNU, BSD, Apache, etc. In nearly all these cases the software can be used without paying a fee. It should be noted that sometimes large organizations distribute the source code, such as Apache, Open Office, Mozilla, etc.

Something else to consider is that you can modify open source software to add capabilities not originally in the software.

Closed source software on the other hand refers to software which is owned by someone (or an organization) and often, the only way to get hold of the software is through purchasing a physical product or a digital product from retailers, re sellers or the owner's website. Access to the source code is an impossibility. Based on its license conditions, you cannot download or modify its source code. You can't even verify the code integrity as to ensure that no malicious code was deposited that could undermine its users.

Most of the code used in the Blockchain Technology industry are Open Source with their source code kept in public repositories like GitHub, BitBucket or GitLab, for anyone who has good enough knowledge about coding, to inspect and improve upon or even use for his own entirely different purpose. I personally love and support open source software initiatives.

Permissioned vs Unpermissioned Blockchain

A permissioned blockchain also known as private blockchains, is a protocol that restricts the actors who can contribute to the consensus of the system state. In a permissioned blockchain, only a restricted set of users have the

rights to validate the block transactions. A permissioned blockchain may also restrict access to approved actors who can create smart contracts.

Permissionless blockchain or un-permissioned is contrary to what you read above – Here anyone can join the network, participate in the process of block verification to create consensus and also create smart contracts. A good example of permissionless blockchain is the bitcoin and Ethereum blockchains, where any user can join the network and start mining (confirming transactions).

Now you may wonder what the benefits and disadvantages of each approach are? In a permissionless world, you do not have to prove your identity to the ledger. As long as you are willing to commit processing power to be part of the network and extending the blockchain, you are allowed to play. Any miner who is playing the game by the rule may be able to solve the hash puzzle and verify the block of transactions to win the mining reward (the higher the mining power, better the chances of winning the mining reward).

In the permissioned blockchain world, you need to be an approved actor in the system to participate in growing the chain as well as building consensus. Many of the blockchain consortiums that build private blockchains for financial institutions and other enterprises follow this model.

One other critical difference between these two is the underlying mining model – permissionless blockchains use Proof of Work (PoW) mining where hashing power is offered to build trust. As long as 51% of the nodes are honest players, network consensus is reached. While Bitcoin and ethereum uses PoW mining, some others uses a Proof of Stake model (PoS) for reaching consensus. Proof of stake mining asks users to prove ownership of a certain amount of currency (their “stake” in the currency). Instead of buying computers and electricity for mining in a PoW system, a PoS systems uses the capital to acquire the coins/ tokens that allow you to validate transactions.

Permissioned blockchains do not have to use the computing power based

mining to reach a consensus since all of the actors are known; They end up using consensus algorithms like RAFT or Paxos. There are also other PBFT algorithms that can be used to reach consensus without PoW mining. More on these algorithms later, or see the glossary section.

Blockchain Technology Stack

Digital Tokens/ Cryptocurrencies

The first Digital Currency was bitcoin. It was the first fruit of the blockchain technology. Bitcoin gained main stream public attention in 2008. Nick Szabo had earlier founded an early digital currency known as eCash in 1998 but the project was not successful because the internet was too young and immature to appreciate its key concept. The identity of Satoshi Nakamoto, the brilliant computer programmer who created bitcoin virtual currency, is one of the most compelling stories in technology. In 2008, Nakamoto launched bitcoin with a white paper; in 2011, he vanished, just as the project was hitting its stride, his frequent forum posts and e-mails tapering off to silence. (In his last known correspondence, he told a bitcoin developer that he had "moved on to other things." Bitcoin was created an electronic payment system based on mathematical proof. The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees. When we mention digital currency, virtual currency or cryptocurrency in this book, we are referring to one and same thing.

Smart Contracts

In 1994, Nick Szabo (he proposed the concept of the first smart contracts), a law scholar and cryptographer, realized that the decentralized ledger could be used for smart contracts otherwise called self-executing contracts, blockchain contracts or digital contracts. In this format, contracts could be converted to computer code, stored and replicated on the system and supervised by the

network of computers that run the blockchain. This would also result in ledger feedback such as transferring money and receiving the product or service. Szabo defined smart contracts as computerized transaction protocols that execute terms of a contract.

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way, while avoiding the services of a middleman.

The best way to describe smart contracts is to compare the technology to a vending machine. Ordinarily, you would go to a lawyer or a notary, pay them, and wait while you get the document. With smart contracts, you simply drop a bitcoin into the vending machine (i.e. ledger) and your escrow, driver's license, or whatever drops into your account. More so, smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

Smart contracts are created by computer programmers through the help of smart contract development tools. They are entirely digital and written using programming code languages such as C++, Go, Python, Java. Ethereum has become the most popular platforms for programming Smart Contracts, probably because of the simplicity of its “Javascriptlike” language Solidity. This code defines the rules and consequences in the same way that a traditional legal document would, stating the obligations, benefits and penalties which may be due to either party in various different circumstances.

It must be said however that a smart contract is as smart as the programmer who coded it. The DAO hack experience is an unforgettable case in point. More on this latter.

In its most basic form, a smart contracts gives you:

Autonomy: You're the one making the agreement. There's no need to rely on a broker, lawyer or other intermediaries to confirm. Incidentally, this also knocks out the danger of manipulation by a third party since execution is managed automatically by the network rather than one or more, possibly biased, individuals who may err.

Trust: Your documents are encrypted on a shared ledger. There's no way that someone can say they lost it.

Backup: Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends has your back. Your documents are duplicated many times over.

Safety: Cryptography, the encryption of websites, keeps your documents safe. There is no hacking. In fact, it would take an abnormally smart hacker to crack the code and infiltrate.

Speed: You'd ordinarily have to spend chunks of time and paperwork to manually process documents. Smart contracts use software code to automate tasks, thereby shaving hours off a range of business processes.

Savings: Smart contracts save you money since they knock out the presence of an intermediary. You would, for instance, have to pay a notary to witness your transaction.

Accuracy: Automated contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.

Block Explorers

A block explorer allows you to search and navigate through the block chain. Using a block explorer you can check the balance of different crypto currencies' public addresses, track coin transfer histories, watch how many confirmations a transaction has and get a wide variety of statistics about the network such as the current hash rate and more.

For each block chain, there is a different block explorer. For example, you won't be able to use a bitcoin block explorer in order to examine litecoin

or ethereum blockchain.

What can you do with a block explorer?

Usually the block explorer software will supply some or more of the following:

* A list of a chain's recent blocks
* Transactions in a given block
* Links to the previous and next transaction involving each input and output
* A list of all transactions involving a given address
* Current and historical address balances
* A way to search for blocks, transactions and addresses

How to Examine a Public Bitcoin Address Using the Most Popular Block Explorer Today, Blockchain.Info:

Just paste any public address (wallet address, or transaction ID) into the block explorer and you can see how many bitcoins the wallet holds and its recent transactions. If you click on a specific transaction you will see details about this transaction such as when it was received, the number of confirmations it has or when it is estimated to be confirmed, the inputs and outputs of this transaction and how many bitcoins were transferred.

List of 8 Popular Cryptocurrency Block Explorers (Every Decentralized Cryptocurrency has its Blockchain. It's a Requirement).

Blockchain.info: The most popular bitcoin block explorer today. The company also provides a very popular (and recommended) bitcoin wallet service.

Blockr.io: A multi-currency block explorer. Used not only for bitcoin but also for litecoin, peercoin and more.

Blockexplorer.com: Perhaps, not as well designed as the others but definitely the longest existing block explorer. The website supplies the basic information for all bitcoin transactions and wallets.

Insight.is: The Insight REST API provides a convenient, powerful and simple way to read data from the bitcoin network and build your own services with it.

etherscan.io: Ethereum Block Explorer

etherchain.org: Ethereum Block Explorer

gastracker.io: EtherClasic Explorer

Etcchain.com/explorer: EtherClasic Explorer

Decentralized Applications -DApps.

Decentralized apps are a new type of software program designed to exist on the Internet in a way that is not controlled by any single entity. Where bitcoin is a decentralized value exchange, a decentralized application aims to achieve functionality beyond transactions that exchange value. Many types of decentralized apps are starting to emerge as blockchain technology continues to progress. More companies and individuals are seeing the potential for what can be achieved in decentralizing not just money but almost any type of computing imaginable.

Decentralized apps potentially represent the next generation of computing. In a completely decentralized world all things occur using peer-to-peer networks and the idea of centralized entities are non-existent. This distributed future is still being designed and built but the early stages of development are looking promising.

An overview of DApps can be found at the following Github repository:
https://github.com/DavidJohnstonCEO/ Decentralized Applications

According to "The General Theory of Decentralized Applications, DApps", a decentralized application or DApp (pronounced dee-app) must meet the following 4 criteria:

1. The application must be completely open-source, operate autonomously, and with no entity controlling the token majority. Changes to the application must be adopted by consensus.
2. Data must be cryptographically stored in a distributed blockchain to avoid central failure points.
3. The application must use a cryptographic token for access to the application and as reward to network supporters.
4. The application must generate tokens according to an algorithm that values contributions to the system.

What Types of DAPPs Exist?

There are currently several categories of decentralized applications but there is no dominant or decided method. The different application types still use blockchain technology, but there are variations that separate them from bitcoin alone.

DAO – Decentralized Autonomous Organization

A DAO is an organization that is able to operate without human intervention and does not depend on a single point of distribution. A DAO is programmed and stored on a blockchain; where its conditions are checked and actions are performed based on the protocol of the network. A DAO is the basis of decentralized applications.

DAOs can have varied levels of complexity depending on the objective of the organization. DAOs can be used to represent all sorts of real-world scenarios including ownership of property, settlement of claims and distribution of funds to name a few examples. A DAO can be organized using

a “contract” which typically involves a set of rules that are defined in code and written to the blockchain of the network for the dApp.

Below Are a few Examples of DApp Technologies:

Ethereum introduces a dedicated blockchain capable of supporting a “Turing complete” programming language. Ethereum allows developers to create their own decentralized applications that “live” on the Ethereum blockchain. The first developer release of Ethereum is available. So, people have started working on applications for this platform.

MaidSafe provides a “proof of resource” mechanism and decentralized data structure for storing files privately or publicly in the cloud. This system cryptographically stores file that are distributed throughout the network for on-demand retrieval by the file owners.

BURST is a system that uses the “proof-of-capacity” mechanism, a hard drive based mining solution for network security. BURST has also incorporated “automated transactions” into the capabilities of the network.

At this point in time, most DApps are still in very early stages of development. There are many opportunities for ambitious developers to stake claims in new territory. The pace at which DApp development is progressing is a testament to the momentum of cryptocurrency development and the movement towards decentralization.

The DApp development space is growing quickly as the security of blockchain based transactions continues to get recognized.

Protocols

In general, a protocol is the special set of rules that nodes in a network use when they transmit information. These rules specify the interactions between the communicating entities.

One example of a protocol used in telecommunications is Transmission Control Protocol (TCP), which is a set of rules for exchanging messages at the information packet level on the internet. TCP guarantees that the data packets will be delivered and that they will be delivered in the same order in which they were sent. Another example of a protocol is Internet Protocol (IP), which is a set of rules to send and receive messages at the Internet address level—it essentially specifies the format of the data packets on the internet and the addressing scheme.

When discussing blockchains, the term "protocol" refers to the "cryptoeconomic rules" that are enforced by a blockchain in order to maintain distributed consensus across the blockchain's peer-to-peer network.

Cryptoeconomic Rules Are Rules that Govern a Decentralized Digital Economy that:

(1) Uses public key cryptography for authentication.

(2) Has economic incentives to ensure that the rules are followed.

For example, in the case of Bitcoin's blockchain, it has financial incentives that are provided to the miners for validating every bitcoin transaction and in turn, securing the network.

The ultimate dream of cryptocurrency developers is that we can take advantage of this blockchain technology to build new and improved communication protocols from the ground up. Protocols being developed for cryptocurrencies have the potential to solve problems with centralization that have plagued the Internet since the first dial-up modem whirred and beeped into action.

Most tokenized cryptocurrencies have their own protocol. There is the bitcoin protocol, ethereum protocol etc. Remember the ultimate purpose of a protocol is simply to specify rules for communication between nodes. Some protocols have intrinsic tokens, some don't.

So essentially, there are two types of protocols:

1. Ones which have an intrinsic token associated with it, that helps to create economic incentives that drive a network.

2. Ones which doesn't have a token that drives financial incentives but are simply used as a communication protocol between nodes (Note: these types of protocols CAN still have a token associated with it—e.g. to represent membership in the network, shares on an open market, etc. The difference is that they are not used to drive some economic incentive.)

I will highlight more on this in a later chapter.

Blockchain Application/ Use Cases

The transparent and decentralized nature of the blockchain network enables the development of a non-refutable and unbreakable records of data, which is the fundamental feature that most companies are exploring and applying to their core businesses. In other words, substantial **decrease of intermediaries**, **fraud** and **access to real-time information** without manipulations. Also, there would be a **decrease in bureaucracy** burden improving the time invested in these processes. As a consequence, this has big implications for business and anyone looking to seize opportunities in the blockchain technology revolution to create Trans generational wealth as never seen before now.

One sector that will be greatly impacted is the financial services industry, as we shall see in this section.

The **World Economic Forum's** analysis of Distributed Ledger Technology (DLT) a.k.a The Blockchain Technology, yielded six key findings regarding its implications on the future of financial services.

The Key findings are;

DLT has great potential to drive simplicity and efficiency through the establishment of new financial services infrastructure and processes.

DLT is not a panacea; instead it should be viewed as one of many technologies that will form the foundation of next generation financial services infrastructure.

Applications of DLT will differ by use case, each leveraging the technology in different ways for a diverse range of benefits.

Digital Identity is a critical enabler to broaden applications to new verticals; Digital Fiat (legal tender), along with other emerging capabilities, has the ability to amplify benefits.

The most impactful DLT applications will require deep collaboration between incumbents, innovators and regulators, adding complexity and

delaying implementation.

New financial services infrastructure built on DLT will redraw processes and call into question orthodoxies that are foundational to today's business models.

Many have the opinion that the blockchain technology will do to banks what email did to post offices.

However, many industries are finding new ways to use the blockchain technology to solve problems and reduce cost. As a consequence, startups are springing up in droves, looking to catch in on new opportunities. Find below a list of some interesting use cases across multiple industries being disrupted by the blockchain technology and awesome startups within each use case. Will you sit back and watch or stand up to be counted?

Peer to Peer Lending

Peer-to-peer economy facilitated by blockchain has been among the examples for the technology's disruptive and innovative potential. However, using bitcoin to send money around the world is slightly different from using bitcoin as a currency. Peer-to-peer payments and lending belong to the first case. By eliminating the intermediaries, the blockchain can enable cheaper cross-border remittances and; therefore, enhance the spending power of recipients.

Interesting startups in this field:

- **Abra**: Abra has built the first global, peer-to-peer, digital cash, money transfer App using Blockchain technology for secure money transfers and payments while protecting the value of deposits in local currency.
- **BTC Jam**: It provides a peer-to-peer lending service where people from around the world connect to borrow and lend using bitcoin. It is allowed to users in countries that lack a local credit score system to receive loans, based on an in-house credit-scoring algorithm.
- **Bitbond**: A global peer-to-peer lending platform for Bitcoins. Borrow Bitcoins or earn interest on your Bitcoins on our international marketplace.

- **Circle**: A peer-to-peer payments technology company utilizing Bitcoin and traditional fiat currencies.
- **Plutus**: A true peer to peer exchange network on the blockchain. PlutusDEX runs as a Dapp on the Ethereum blockchain.
- **StartUP Bits.Fund**: A Nigerian based peer-to-peer lending platform based on Ethereum token. Borrow Ethereum, or earn interest on your Ether on the local marketplace.
- **Humaniq:** Humaniq is a simple and secure mobile app, delivering financial inclusion solutions to the 2.5 billion unbanked / 1 billion underbanked globally. Humaniq brings isolated people into modern markets, creating a new source of growth for the world economy by impacting individual livers.
-

Internet of Things

As blockchains and sidechains proliferate, there are several important implications for the Internet of Things and the development of Smart Systems. For one, blockchain technology could provide a way to track the unique history of individual devices, by recording a ledger of data exchanges between it and other devices, web services, and human users. Examples include; electronic couriers to securely transfer sensitive information, escrow services to transfer ownership rights, or even auto-installation services to verify and push updates to the software governing other Digital-to-analog converters (DACs).

Interesting startups in this field:

- **Chimera-inc:** Chimera connects the Internet of Things to real-time analytics performed on the edge node. It is a hub that links the home network to the cloud and electrical devices around it.
- **Filament:** Filament is building a decentralized IoT stack to ensure that devices can securely communicate and transact value without any siloed infrastructure. Filament builds sensors (called “Taps”) that are used by companies such as Amazon and SpaceX.

Voting and Election

Existing electronic voting systems all suffer from a serious design flaw: They are proprietary, that is, centralized by design, meaning there is a single supplier that controls the code base, the database, the system outputs and supplies the monitoring tools at the same time. The lack of an open-source, independently verifiable output makes it difficult for such centralized systems to acquire the trustworthiness required by voters and election organizers. The blockchain works as a secure transaction database, to log votes and audit vote results in a trustworthy way.

Interesting startup in this field:

- **Follow my Vote:** *Follow My Vote* aims to change the way we vote, becoming the world's first secure open-source online voting software based on blockchain technology.

Currency exchange and Remittance

Multiple issues such as high transfer cost, limited money distribution methods, limited brand options, limited ways to deal with money, etc. hold enormous potential for innovation in financial services. The Currency exchange and remittance use case is perhaps the most advanced of the list since it has been implemented worldwide [5]. Dozens of large financial institutions, including many of the world's major banks, have already launched initiatives to explore blockchain's potential.

Interesting startups in this field:

- **Coinbase**: A bitcoin exchange company that operates exchanges between bitcoin and fiat currencies in 32 countries, and bitcoin

transactions and storage in 190 countries worldwide.

- **Ripple**: Ripple's distributed financial technology allows for banks around the world to directly transact with each other without the need for a central counterparty or correspondent.
- **BitPesa**: A universal bitcoin payment and trading platform for Africa.
- **Chain.com**: Chain partners with leading financial institutions to build blockchain networks. Chain solutions enable institutions to design, deploy, and operate blockchain networks that can power any type of asset in any market.
- **Stellar**: A new payment protocol and currency, aims to bridge the gap between cryptocurrencies and fiat by allowing easy and instant exchanges between currencies.
- **Paxful:** Paxful is the leading peer to peer marketplace where regular people can buy bitcoin instantly. Put a single line of code on your blog, website, app or social network post and watch as your visitors buy bitcoin in Paxful's widget.
- **CEX.IO:** CEX is a perfect marketplace for buying Bitcoins in a few clicks. CEX.IO claims to provide the best experience of buying Bitcoins with payment cards on the market.
- **CORION:** Corion (**C**apital **O**ptimized **R**eward **I**ncentive **O**nline **N**etwork) is a multi-functional. Platform for businesses and individuals to join and build a worldwide decentralized network, based on mutual benefits, simplicity, security, cost-effectiveness, speed, and a stable means of payment.

Collaborative transport

Smart transportation is about maximizing already-existing infrastructure and resources rather than adding new ones. Better use of existing resources creates affordable transportation without the need for more roads or vehicles.

Real-time ridesharing is the key, enabling people with private cars to share their journey with others traveling in the same direction. What blockchain adds on top of this is the possibility to put together users without any middlemen thanks to decentralized platforms. Smart Contracts will also enable new ways of settling payments for users and riders.

Interesting startups in this field:

- **La'Zooz**: A Decentralized Transportation Platform owned by the community and utilizing vehicles unused space to create a variety of smart transportation solutions. By using cryptocurrency technology La`Zooz works with a "Fair Share" rewarding mechanism for developers, users and backers.
- **Arcade City**: the groundwork for a true decentralized ridesharing service — what some are now calling the 'Uber killer'. It cuts out the corporate middlemen and make government regulations obsolete by transparently providing rider and driver with clear information about the other party to each transaction, including a strong reputation and ratings system where riders and drivers 'level up' after community-vetted good behavior on the platform.

Decentralized Markets

Decentralized markets are about to kill e-commerce because it will be possible for any two people on the planet to trade with one another without depending on any institution. For instance, eBay/Amazon users and sellers won't make much sense after this field is fully disrupted. On the other hand, the possible scale of blockchain in this field will bring e-commerce to countries that still have not experienced what these traditional marketplaces have brought to industrialized nations.

Interesting startups in this field:

- **Open Bazaar:** Decentralized marketplace for instantly trading goods

and services with anyone using Bitcoin.
- **Slock.it**: It disrupts the billions dollar disruptors by enabling anyone to rent, sell or share their property without middleman.

Proof of Authorship and Ownership

In order to express the authorship of any kind of document (paper, photos or audio/video recording) something called proof of existence may be used. Time stamping data in an unalterable state while maintaining confidentiality is perfect for many fields, especially legal and artistic applications. This simple method allows anyone to store a hash of any document into the blockchain, thus proving it existed at the time when a particular block was mined. The author's name or other identifier would be included into the document, making it clear that he knew about it back then. If nobody proves the possession/familiarity with that particular file/work dated before, the author should be able to claim his rights.

Interesting startups in this field:

- **Proofofexistence**: Anonymously and securely store an online distributed proof of existence for any document.
- **Blocktech**: An open-source standard in active development to allow users to publish and distribute original content themselves, from music to videos to feature films, 3d printable inventions, recipes, books and just about anything else.
- **Clipperz**: A tool to protect and manage intellectual property on the blockchain. A place where you can share your works knowing that authorship and copyright are secured. And where selling a digital product is as easy and secure as selling a physical one.
- **Stampery**: Create an immutable record of existence, integrity and ownership of your documents, business processes and communications leveraging the Blockchain.
- **Bitproof**: BitProof protects people's creations from being stolen and

provides the ability to create legal proofs of documents in less than a minute over the blockchain.
- **Blockai**: A proof of ownership certificate which can legally help prove you are the owner.

Energy Consumption

New energy initiatives such as home power generation and community solar power are filling in gaps of power supply across the world. Solar panels are connected to the internet with technology provided by startups such as Filament (see IoT blockchain use case), allowing traditional electronic devices to be connected online. Anonymous certificates are created and can – in theory –subsequently be sold to anyone who wishes to subsidize solar energy.

Interesting startups in this field:

- **LO3**: Tools and develop projects to support and accelerate proliferation of the distributed energy, utilities and computation sharing economy of the future.
- **Brooklyn Microgrid**: A small-scale, community microgrid that will allow local residents to buy and sell the energy they produce from rooftop solar power installations, using the existing energy infrastructure and the blockchain.
- **Solar Change**: It gathers a network of services and applications meant to improve and increase the use of solar energy worldwide. They introduce SolarCoin – a revolutionary reward program which is coupled to the production of clean solar energy.

Trustworthy Endorsements and Identity

True identification should be readily available to those who need it, and a publicly distributed ledger can help. On the other hand, enabling authenticity of a review through trustworthy endorsements for employee peer reviews is possible with blockchain. Identity is who you are and what others think of you (which is in many cases a more honest view than what you'll say about yourself).

Interesting startups in this field:

- **ShoCard**: stores your identity onto bitcoin's blockchain so that you can prove your identity whenever you need to.
- **UniquID**: A decentralized, blockchain-based, software for identity and access management of connected things.
- **Traity**: It offers a way to build, protect and manage your reputation. Traity backs up your reputation on the blockchain.
- **Onename**: The global database for people, companies, websites and more. Decentralized, privacy-centric, and blockchain-secured.
- **The World Table***:* A decentralized reputation platform supported by an online community and an open-source project.
- **ArtByte**: Artbyte is a person to person digital currency. With artbytes, art lovers can now support their favorite artists directly

Data Storage

Current cloud storage services are centralized — thus users must place trust in a single storage provider. With the Blockchain, this can become decentralized. While some traditional industries such as Banking have already proved to benefit from decentralized data storage, some fields such as the health industry are about to experience a disruptive change. Consider all the sensitive information that is associated with health: identity, diseases, treatments, payment, etc. that could be privately secured and stored, thanks to blockchain!

Interesting startups in this field:

- **Tierion**: Has built a platform for data storage and verification using the bitcoin blockchain.
- **Peernova**: Builds immutable systems for large-scale, commercial applications.
- **NXT**: A decentralized data storage system. Own your data.
- **Filecoin**: A data storage network and electronic currency based on Bitcoin.
- **Sia**: Sia splits apart, encrypts, and distributes your files across a decentralized network. Since you hold the keys, you own your data. No outside company can access or control your files, unlike traditional cloud storage providers.

Custodian Services

Disintermediation is a big threat to the industry particularly in the post-trade ecosystem. If a blockchain can replicate a settlement and custody infrastructure at lower costs then ownership could be transferred without the need for expensive intermediaries. As an example, if the blockchain held the registration details of each trade, there would no longer be a need to distinguish between custodian, CSD (central securities depository) and registrar.

Interesting startups in this field:

- **IBT** (Formerly Fundrs.org): Helps you safeguard your letter of credit, contracts digitally based on blockchain technology. It solves the risk of non-delivery for buyers and the risk of non-payment for sellers online. But most importantly, at a fraction of the cost of a traditional service.

Smart Contracts

Smart Contracts are self-executing contractual states, stored on the blockchain, which nobody controls and therefore everyone can trust. An important feature of a smart contract is the ability to reduce risk through non-discriminatory execution. The lack of a central counterparty agent can enable such contracts to service markets with greater efficiency.

Interesting startups in this field:

- **Mirror**: Mirror is a contracts platform and data provider that democratizes access to financial markets, developing a smart contracts platform to enable P2P trading.
- **UbiMS**: This is developing the Inter-Supply-Chain-Net (ISCN). The ISCN is an IT portal powered by a blockchain that executes an order fulfillment utilizing a patented [3D] supply chain process system to distribute products from the manufacturer to the consumer in the most efficient way possible.
- **Blockstream**: Develops new ways to accelerate innovation in crypto currencies, open assets and smart contracts.
- **Hedgy**: Develops your use case and deliver smart contract enabled distributed ledger systems.

Online Gambling and Gaming

Surprisingly, a large percentage of Bitcoin transactions are gambling-based. The speed and anonymity bitcoin offers has made the cryptocurrency ideal for people looking to wager safely and has given sports gamblers an alternative to traditional online books. Usually players have to go through a tedious process sending and receiving their money from gambling sites leaving a big area for improvement.

Interesting startups in this field:

- **SatoshiDice**: The leading bitcoin gambling site in terms of amount

wagered which uses the digital currency Bitcoin.

- **Augur**: Combines the magic of prediction markets with the power of a decentralized network to create a stunningly accurate forecasting tool – and the chance for real money trading profits.
- **Deckbound**: Creates an ecosystem of technology and services where players and content creators can build and share gaming assets across multiple games and systems in a secured and open environment.
- **SuperDAO**: SuperDAO is an Efficient, tiered & reputation based, Ethereum decentralized and autonomous organization governance system for incentivized global collaborative management of disruptive, economical viable DApp ventures. Their pilot project is ***Pokereum poker*** (formally known as nxtpoker) a decentralized poker project, that uses an EVM based smart contract, decentralized blockchain and real time communication (RTC) peer to peer framework to solve mental poker problems.

Documents Digitization and Contracts

With the dramatic increase in types of data and respective formats, the need to integrate and share data across systems has become vital. For most organizations, this involves delicate balancing of the processes that move data between systems. Blockchain plays an important role in a holistic innovation and risk management strategy, including concepts of cyber liability, big data and telematics.

Interesting startups in this field:

- **Colu**: Creating, storing and managing digital assets using blockchain technology, a record-keeping tool for online identity and the Internet of Things.

Digital Security Trading

Most investors in public securities never see their stock certificates, so a plan to do away with this is in line where technology is moving in general. Unless you have a room wall papered with stock certificates you will not be missing anything [11]. The untested nature of the trading system is a concern that can be solved by blockchain technology.

Interesting startups in this field:

- **Symbiont**: A provider of smart securities on the blockchain. The company aims to eliminate many of the inefficiencies and the opaqueness that have developed on Wall Street by utilizing the speed and security of cryptographic distributed ledgers known as blockchains to enable faster markets that are more efficient, and exhibit lower costs with increased liquidity, transparency and security.
- **Secure Asset Exchange**: Allows issuers and investors to utilize secure decentralized infrastructure to its full potential, by offering investors and issuers a suite of easy to use web-based tools to interact with an exchange infrastructure that nobody controls and therefore everyone can trust.
- **Bitshares**: Provides a high-performance decentralized exchange, with all the features you would expect in a trading platform. It can handle the trading volume of the NASDAQ, while settling orders the second you submit them.

Luxury goods

The afterlife of goods can be dramatically changed through the existence of a full lifecycle record and supply chain tracking, now possible thanks to blockchain technology. Although luxury objects such as gold, diamonds and watches are interesting examples, the disruptive use of this technology within identification and authentication lies in the health industry. According to Interpol, more than 200,000 people die worldwide annually from counterfeit

anti-allergy drugs alone. Blockchain helps anti-counterfeit in very meaningful ways.

Interesting startups in this field:

- **Everledger:** Everledger provides an immutable ledger for diamond identification and transaction verification for various stakeholders, from insurance companies to claimants and law enforcement agencies. Everledger provides new methods of financing and insuring diamonds, as well as combating fraud, by providing an application for various stakeholders in the diamond pipeline.
- **ChainLink**: Uses blockchain technology to verify and validate the authenticity and title of real world items.
- **Blockverify**: A blockchain based anti-counterfeit solution in different industries.
- **Provenance**: It enables every physical product to come with a seamless digital 'passport' empowering transparency and trust. Preventing the selling of stolen or fake goods and creating an audit able account for the journey behind all physical products.

Governments Services

Blockchains are enormous catalysts for change that affect governance. It could improve transparency and check corruption in governments worldwide. In fact, Estonia has become notable for its e-government system, which was established in 1997. This is enabled by a chip-embedded ID card that gives the nation's citizens access to over 1,000 e-government services, such as filing taxes and voting, almost instantly and via just one website.

Interesting startups in this field:

- **Bitnation**: A blockchain-based "Governance 2.0" initiative with a collaborative platform for DIY governance.
- **Stampery**: An immutable record of existence, integrity and ownership

of your documents, business processes and communications leveraging the blockchain.

- **Shocard:** A digital identity that protects consumer privacy and is as easy to understand and use as showing a driver's license.

The fact remains that blockchain technology will disrupt every industry heavily inter-mediated, especially

(1) Those industries inter-mediated by legacy gatekeepers, or

(2) Those entities which represent a potential conflict of interest via-a-vis the parties for whom it is facilitating transactions.

The most obvious example of the former is international remittance. Regarding the latter, the blockchain will disrupt industries like energy and communications infrastructure, which are especially vulnerable to political interventions by the state. The blockchain will also radically disrupt IoT by enabling scale able architectures for the so-called economy of things.

The blockchain represents a huge opportunity for entrepreneurs to find new ways to leverage blockchain technology in order to create better systems and services for various organizations.

For example, the blockchain technology enables ***Bitwage***, a payroll company, to process international payroll in minutes instead of days through the traditional banking system. MPESA in Kenya has made waves with its blockchain solution for small payments in many African countries. The use-case list above, nevertheless, is not exhaustive but shows what a lot of companies are already doing with this nascent technology.

Your startup too can join the list. All it takes is to seize the opportunity offered in the blockchain ecosystem!

Preparing your Organization for Blockchain Technology Transition

As we have already seen so far, there is a growing realization that blockchain is bringing a radical shift in almost every field of human endeavors, just like the internet did. The journey is likely to be long and the outcome is uncertain, but a consensus is forming, and that is the real deal. Disregarding this wave of change is a huge risk.

Collectively, the tone of conversations has shifted from "Is this worth exploring?" to "How do we best engage?"

Time to Get off the Sidelines

• Many Chief Executives have taken a wait-and-see approach, under the assumption that any eventual cost savings or opportunities will flow downstream.

I believe this is a mistake. Do not join that group.

• Early engagement is essential for executives to drive prioritization of the right issues and use cases; competitive advantage can be gained from working with the right partners early on to develop real world solutions.

The following are the recommended steps the CEO, COO or CTO should take to prepare their organizations for the blockchain transition:

Role 1: The CEO.

You need to outline the vision for how the organization engages with and adopts blockchain. The priority placed on blockchain will depend on the size and nature of your firm, and this needs to be understood. From this basis, the CEO can mobilize the management team and make the right level of investment.

Five Suggested Actions Steps:

Assess and understand the potential impact of blockchain on your organization.

• Are you personally well-educated on blockchain?

• What level of change can blockchain bring to your business and organization?

• Do you understand what can accelerate change? What are the hurdles/ open questions? What is the timing?

Outline the longer term vision and the ambition for your organization.

• Where do you want to be; a first mover, a fast follower or wait for industry solutions?

• What level of resourcing do you want to commit (e.g., investment budget, management bandwidth)?

• What areas of impact do you want to focus on (e.g., technology development, regulatory reporting)?

• Are there strategic partners you intend to engage (across your competitor and ecosystem community)?

Determine where blockchain falls on the priority scale for your leadership team, especially via-à-vis other innovative technologies.

• Does blockchain make the top five focus areas in the next five years? Top 10?

• If a potential Top 10 priority, who is leading blockchain thinking for your organization?

• Do you need to spend significant resources now, or can you wait a few more years?

Encourage open and trans formative thinking, particularly among young tech teams.

• What is the forum for blockchain to be discussed and ideas to be raised with you?

• Are you allowing creative liberty and time for senior leaders to explore the radical transformative impact of blockchain technology?

• Are you driving the right balance between thinking and learning about blockchain as well as executing on potential ideas?

Develop an external engagement approach.

• Are there select partners in your peer group that may allow you to share thinking and build use cases together?

• Which consortia partnerships may make sense for you to pursue?

• How public do you want to be on your ambition level?

How important is it for you to be perceived as a front-runner among your peers?

Role 2: The CTO

You need to lead understanding and development of blockchain capabilities as part of the broader FinTech agenda. This includes setting up the right teams internally and working with external parties. The CTO needs to ensure the advancement of blockchain expertise on the management team and within the organization.

Five Suggested Actions:

Lead internal understanding and awareness campaign around blockchain.

• Do your colleagues (e.g. COOs) understand the distributed ledger technology (DLT) and its potential applications?

• Are the right leaders following the development of the technology and protocols?

Identify the emerging experts across the organization.

• What is the forum your teams have to raise DLT-related ideas to you?

• Are technology teams encouraged to contribute actively (e.g., hackathons, code sprints, blockchain Conferences)?

• Are responsibilities clear across monitoring market developments, engagement, internal communication, driving use cases?

• Do you need to make investments in IT capabilities, skills or training?

Determine if/ when the creation of a blockchain lab for your organization makes sense.

• Are there potential use cases that your organization wants to drive? Is a consortia model appropriate?

• Are efforts focused on identifying use cases from real pain points (and not finding a problem for blockchain to solve)?

• Do you have the right mix of technical understanding and business familiarity?

Review any long-term technology decisions that can be impacted by blockchain.

• Are you making technology decisions that can be heavily impacted by blockchain?

• What technologies could make today's decisions incorrect?

• What are the long-term implications of other disruptive technologies (e.g., machine learning, robotics, data analytics) converging with blockchain development?

Engage with external vendors, and follow technology advancements in the space.

• Who are the key vendors that you want to closely follow as this space advances?

• What industry events and conferences do you want to participate or engage in?

Role 3 : The COO

He needs to understand blockchain applications and ensure they make up part of a coherent target operating model. The COO is responsible for extracting the benefits for the organization, as well as fitting work alongside existing transformation initiatives. The COO also needs to be the pragmatist, preventing disruption to the firm's day-to-day ability to do business.

Five Suggested Actions:

Bring the business process and controls to view potential blockchain applications.

• What blockchain enhancements can dramatically alter your current businesses processes?

• Which of your processes could most benefit from blockchain? What is the potential impact?

• What processes could be rewritten or made redundant due to blockchain technology?

Partner with the CTO on determining if/ when a blockchain lab makes sense for your organization.

• Who is driving and leading the business case development for your organization?

• Is blockchain thinking and development led solely by the technology organization?

• Are you assessing the way competitors are approaching the technology?

Future-proof long-term operating model decisions that may be impacted by blockchain.

• Are you making operations decisions (e.g., location strategy) for the future that can be heavily impacted by blockchain?

• Could any outsourcing or vended solutions become obsolete?

• What capabilities will require investment in the long term?

Identify partners across the ecosystem that are active and engage them.

• Who are the key business partners (e.g., custodians, clearing partners, FinTech startups) that you want to work with on blockchain?

• Are any competitors experimenting with use cases? If so, how do you want to engage/ respond?

Prioritize use cases to follow/ monitor, and ones to lead and develop yourself.

• Are there select use cases you want to incubate and lead for your organization or business?

• Of the different industry use cases, what are the top ones that you want to monitor?

• When do you plug in to new deployments to maximize savings and other benefits?

The consequences of blockchain will vary for individual organizations — every firm's vision and approach is a unique decision.

It is my belief that distributed ledger technology is not only credible, but creates opportunities for executives and have the potential to change the way they structure and do business. Just as it was impossible to predict the impact the internet would have on financial services, it is impossible to know with certainty how businesses will look or operate when distributed ledgers and cryptographically secured digital assets become the everyday norm. However, recognizing the impact that FinTech innovation continues to have on industries, it is pragmatic to be well-informed and organized in other to unlock economic advantage in an increasingly digital world.

The Dark or Deep Web and Digital Currency Anonymity

The deep web *(a.k.a. the darknet or dark web)* is famous for its black markets, where intrepid shoppers can use Bitcoin and other cryptocurrency to purchase everything from drugs to guns to stolen credit card details over the internet anonymously. The very definition of the deep web is that it contains all of those hidden websites that you won't find in the Google search results. If you have ever wondered how to access these dark web markets and how to buy things from them then read on.

One thing that may surprise you when you first access the Internet's famous black markets is that these are not the kind of *'anything goes'* free for all that you may have seen portrayed in popular culture. Yes, you can use them to buy illegal items, but all of the main marketplaces have rules about what vendors are allowed to sell. In fact, you will find that the most popular marketplaces often seem to be the ones with the strictest rules. You will not see vendors selling poisons, explosives, videos depicting violence, or anything to do with weapons of mass destruction. Some marketplaces also ban guns and other 'lethal weapons', as well as stolen data such as hacked accounts or stolen credit card details. By far the most common thing you will find is drugs, including recreational drugs like cannabis and ecstasy and prescription medicines. You will also find things like counterfeit clothing, accessories and jewelry, and lot of legal items such as e-books and guide, as well as self-defense products such as pepper spray, and software for helping people protect their privacy and stop internet spying.

Another thing that you should be aware of is that many of these marketplaces have downtime. If you click a link to visit a dark web market and it is offline don't panic – it is probably temporary. Yes, these markets do

come and go as they may be shut down by authorities or the administrators may disappear, but they also suffer from a lot of temporary outages due to attacks from other market operators, maintenance, or the side-effects of security measures.

Bitcoin has a reputation in the public imagination for being an anonymous digital currency, like an internet equivalent of physical cash, but that is not entirely correct. *Bitcoin is pseudo-anonymous.* By analyzing the activity which is visible to anybody on the public blockchain an observer may well be able to link your personal identity with all of the wallets you use and therefore your entire transaction history. In a way, this makes bitcoin even less private than a bank account.

Fortunately there are things you can do to improve this situation.

Use disposable wallet addresses.

Bitcoin addresses are not meant to be permanent locations for everything you do. Instead, it will enhance your financial privacy if you view addresses as disposable invoices – each time you are going to receive a payment you should create a new address specifically for that purpose, and then never use that address again afterwards.

Most wallets today will take care of this for you, automatically creating a new address each time you want to receive a payment, but it doesn't hurt to be aware of this issue.

Use Digital Currency Mixing Service.

You can further enhance your privacy by using a mixing service. You can use this when you send a payment to somebody, when you are sending coins to your wallet from the site you bought them on, or you can even send money to another address you own through a mixing service in order to 'launder' it. This works by simply mixing up your coins with a large number of other coins from other sources before sending them out the other side. By doing

this, it becomes difficult or impossible for an observer to link specific payments into the mixing service with specific payments coming out of the mixing service.

One popular and reasonably priced mixing service is offered by CoinMixer.se, but there are also many others about so if you like to shop around then a bit of Googling may be in order – just be careful to check for review though, because there are a couple of scam sites out there which claim to be mixers but actually steal your coins.

Stealth Addresses

Stealth addresses are a reasonably new feature which allows users to generate a new public address to represent any regular bitcoin address. This means that you can then send money to this new stealth address without anybody knowing the true destination of the funds. You do need a wallet which supports this feature in order to use it, and at the time of writing it has not been widely adopted.

Taint Analysis

If you have used a coin mixer then you can check how well its privacy services are performing with a taint analysis. This shows which addresses have sent coins to your address and is a good way to see whether mixing services are performing to your expectations. There are plenty of different service that do this online, so if one is not working well you can always choose another.

You can perform a taint analysis using the Blockchain.info website. Here is an example link, just replace the BTC address with your address in the URL to perform your own taint analysis: https://blockchain.info/taint/1dice6GV5Rz2iaifPvX7RMjfhaNPC8S

This will perform a kind of forensic test to see which addresses it thinks probably did send coins to the address you are checking. You can, for

example, enter the address given to you for a marketplace site to check whether any observer would be able to tell whether your personal wallet sent coins to this address.

If you do not want to use any of the above mentioned methods to conceal your transactional identity, then chose from any of the following three cryptocurrencies that have unrivaled reputation for anonymous use.

1. **Zcash** transactions are untraceable because they use an encryption called zk-SNARK. The transaction metadata within the network is encrypted, and zk-SNARKs are utilized to stop double spends.

2. **Monero** is another strong competitor in the land of anonymous cryptocurrency that uses a method called CryptoNote. Monero was derived from bytecoin, an early altcoin. There are some significant differences compared to both bytecoin and bitcoin within the monero architecture such as target block time, and emission speed. Monero offers an opaque blockchain with a system called viewkey.

3. **Dash** is an open source digital currency, released in 2014, formerly known as Darkcoin. The network uses darksend to help anonymize the transaction process by mixing coins. The network takes in transactions by combining identical inputs from multiple users into a single transaction with several outputs.

So why did we go through this long part, making big deal of anonymous cryptocurrency use and the dark web?

It’s because the demand for privacy will continue to rise and the blockchain technology seem to have given that initiative wings to fly. The general idea is to achieve:

- Untraceability: Make it infeasible to learn anything about the history of a coin.
- Sender-Anonymity: Make it infeasible to link two payments to the same sender.
- Receiver-Anonymity: Make it infeasible to link two payments to the same recipient.
- Hidden Amount: Make it possible to hide the value of a transaction.

But law enforcement agencies and anti-fraud organizations need not worry as there are also deeper technologies that are available today that can easily unveil that which was veiled.

All they need do is to “ask how?”

Cryptocurrency, Digital Currency, and Virtual Currency:

What is Really the Difference?

Cryptocurrency is both digital and virtual currency that is created based on some cryptographic algorithm (Sha-256, Scrypt, etc). Bitcoin, Litecoin, and altcoins are all cryptocurrencies. The key thing here is Cryptography and perhaps decentralization. Some cryptocurrencies may not be decentralized though.

Digital Currency is currency that specifically exists in the digital space, meaning that it maps to some digital storage, likely a hard drive somewhere. It is a subset of a physically existing currency, like US Dollar, Nigerian Naira, or British Pound. It includes any currency that is transferred digitally. Any money based in 1's and 0's meets this definition. Digital currency, however, is connected to the traditional banknote money that the government owns.

Virtual Currency on the other hand are currencies that exist only in the virtual world. Outside that world, they do not exist and they are not tied to any physically known currency. In this category, we can list Perfect Money, E-gold, and Liberty Reserve etc.

Money and Currency

The 3 Main Functions of a Currency

1. What is a medium of exchange?

• A more efficient way to exchange products and services than the barter system (that otherwise
requires a "double coincidence of wants."

• In this regard, money serves the role of an *intermediary* between the products or services that
people want to trade

What makes a good medium of exchange?

• *Durability*: Metals/ gems vs. tobacco/ chocolate

• *Transportability*: Paper money/ electronic registers vs. metals / gems

• *Divisibility*: Metals/ paper money vs. cattle

• *Non-counterfeitability:* A long-standing problem for almost all currencies

• *Fungibility*: Each unit is identical to others in its characteristics and functions. Paper money vs.
cattle/tobacco/cowrie shells

Unit of Account

What is a unit of account?

A standard *measurement* of the value of goods, services, economic activities, assets and liabilities.

• A common unit of account is what allows us to compare.

• The value of 10 lemons vs. 1 book.

• The financial results of a furniture manufacturer with those of an internet portal.

• The size of the economy of Lagos with that of New York City.

Stability: Stability of the value of the unit of account makes it more useful as a unit of account.

In inflationary currencies, for example, over long periods of time, results are not comparable, leading to the need to use *nominal* (actual) vs. *real* (inflation-adjusted) values in order to make measurements comparable again.

Does the Unit of Account have to be the same as the Medium of Exchange?

No! But usually it is.

Some exceptions:

Unidad de Fomento (UF) in Chile: A national indexed unit of account used to adjust for inflation.

External currency pegs: In high inflation countries, merchants have been known to post prices in dollars or other stable currencies (the Unit of Account) but to settle in local currency at the current exchange rate (the Medium of Exchange).

Store of Value

What is a store of value?

A store of value is a mechanism by which wealth can be ***saved*** and retrieved in the future with

some predictability about its future value.

Store of value is not a function solely of currencies, but of assets in general.

As all asset prices have greater or lesser degrees of unpredictability, there is no perfect store of
value.

What drives the ability of something to be a ‘store of value’?

Current expectations of stable or predictably knowable future demand for the asset.

Current expectations of stable or predictably knowable future supply of the asset.

Notable Stores of Value:

Gold / Silver / Diamonds.

Reserve currencies and/or the bonds of reserve currency nations.

Stocks / Bonds / Real Estate.

Bitcoin/ virtual currencies, as unstable as they seem, are the kind of money that works in an unstable world, which is the only kind of world that we all know of, is a good store of value, unit of account, and medium of exchange, to the extent that these terms make sense amid great uncertainty.

Cryptocurrency and how Does it Work?

Cryptocurrency is a digital currency that uses encryption (cryptography) to generate digital tokens or money. Encryption is also used when verifying transactions. Transactions are added to a public ledger – also called a transaction BlockChain. New coins are created through a process known as mining. Hence, cryptocurency is an encrypted decentralized digital token transferred between peers and confirmed in a public ledger via a process known as mining. Most cryptocurrencies are decentralized, and open sourced, meaning that their source codes are available publicly. The monetary system of the currency are also embedded in the code and are beyond the control of any one individual or organization.

One great feature of cryptocurencies is the economic incentives embedded in the code.

For Bitcoin and most altcoins that use PoW algorithm, solving the "Proof of Work" problem requires a lot of computing power and that power costs money. To encourage participants to invest their resources in mining, bitcoin provides a **reward (bounty)** in each successfully mined block (plus the **transaction fees** of the transactions contained in the new block).

When a block is discovered, the discoverers will award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network, in case of pool mining.

Currently, this bounty is ***12.5 bitcoins.***

Based on bitcoin's algorithm, this bounty halves every ***210,000 blocks*** (i.e. approximately every 4 years)

Eventually, the reward will be removed entirely when the limit of 21 million bitcoins is reached asymptotically, by the year 2140.

After that, transaction processing will be rewarded solely by transaction fees.

Cryptocurrency Basics

In order to understand how cryptocurrency works, you'll need to understand a few basic concepts.

Public Ledgers: All confirmed transactions from the start of a cryptocurrency's creation are stored in a public ledger called the blockchain. We have dealt with blockchain in reasonable details in previous sections. The identities of the coin owners are encrypted, and the system uses other cryptographic techniques to ensure the legitimacy of record keeping. The ledger ensures that corresponding "digital wallets" can calculate an accurate spendable balance. Also, new transactions can be checked to ensure that each transaction uses only coins currently owned by the spender.

Cryptographic Hash Functions

Hash functions are extremely useful in digital currencies, and appear in almost all information security applications. It is used basically to check data integrity.

A hash function is a ***mathematical function*** that converts a ***numerical input value*** into another compressed numerical value. The input to the hash function is of ***arbitrary length*** but output is always of ***fixed length***.

Values returned by a hash function are called **message digest** or simply **hash values**.

Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.

In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.

Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.

Secure Hash Function (SHA)

This is a family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, they are structurally different.

SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending on the number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function. Bitcoin and several other altcoins use SHA-256 algorithm to store transactions on its network.

How is Hashing Different from Encryption?

Encryption is a two way function. Data is encrypted with the purpose of being decrypted at a later time. This is the only good way to store or move data in a secured fashion. Private and Public keys are encrypted.

Hashing, however, is never meant to be reversed. It's not meant to be a secure way to store or move data, but is purely used as an easy way to compare two blobs of data. Most cryptocurrencies/ Bitcoin transactions are hashed.

Transactions

A transfer of funds between two digital wallets is called a transaction. That transaction gets submitted to a public ledger and awaits confirmation. When a transaction is made, wallets use an encrypted electronic signature *(an encrypted piece of data called a cryptographic signature)* to provide a mathematical proof that the transaction is coming from the owner of the

wallet. The confirmation process takes a bit of time (ten minutes for bitcoin) while "miners" mine *(ie. confirm transactions and add them to the public ledger)*.

Mining

In simple terms, mining is the process of confirming transactions and adding them to a public ledger. In order to add a transaction to the ledger, the "miner" must solve an increasingly-complex computational problem (sort of like a mathematical puzzle). Mining is open source, so anyone can confirm the transaction. The first "miner" to solve the puzzle adds a "block" of transactions to the ledger. The way in which transactions, blocks, and the public blockchain ledger work together ensures that no one individual can easily add or change a block at will. Once a block is added to the ledger, all correlating transactions are permanent and a small transaction fee is added to the miner's wallet (along with newly created coins). The mining process is what gives value to the coins and in bitcoin, and several cryptocurrencies, is known as a **proof-of-work system**. Some other protocols use different methods to confirm transaction apart from Proof of Work (PoW); such as ***proof of stake (PoS), Proof of Burn (PoB), Proof of Activity, Proof of Capacity***, etc.

Proof-of-Work is system that uses hard-to-compute but easy-to-verify functions to limit exploitation of cryptocurrency mining.

When people mine digital coins and add blocks of transactions to public ledgers, they are typically "cracking" a proof-of-work system by using high-powered computers to solve a mathematical problem. The most well-known proof-of-work function is called ***SHA256***. Bitcoin and several altcoins use SHA256 ***POW*** hash algorithm.

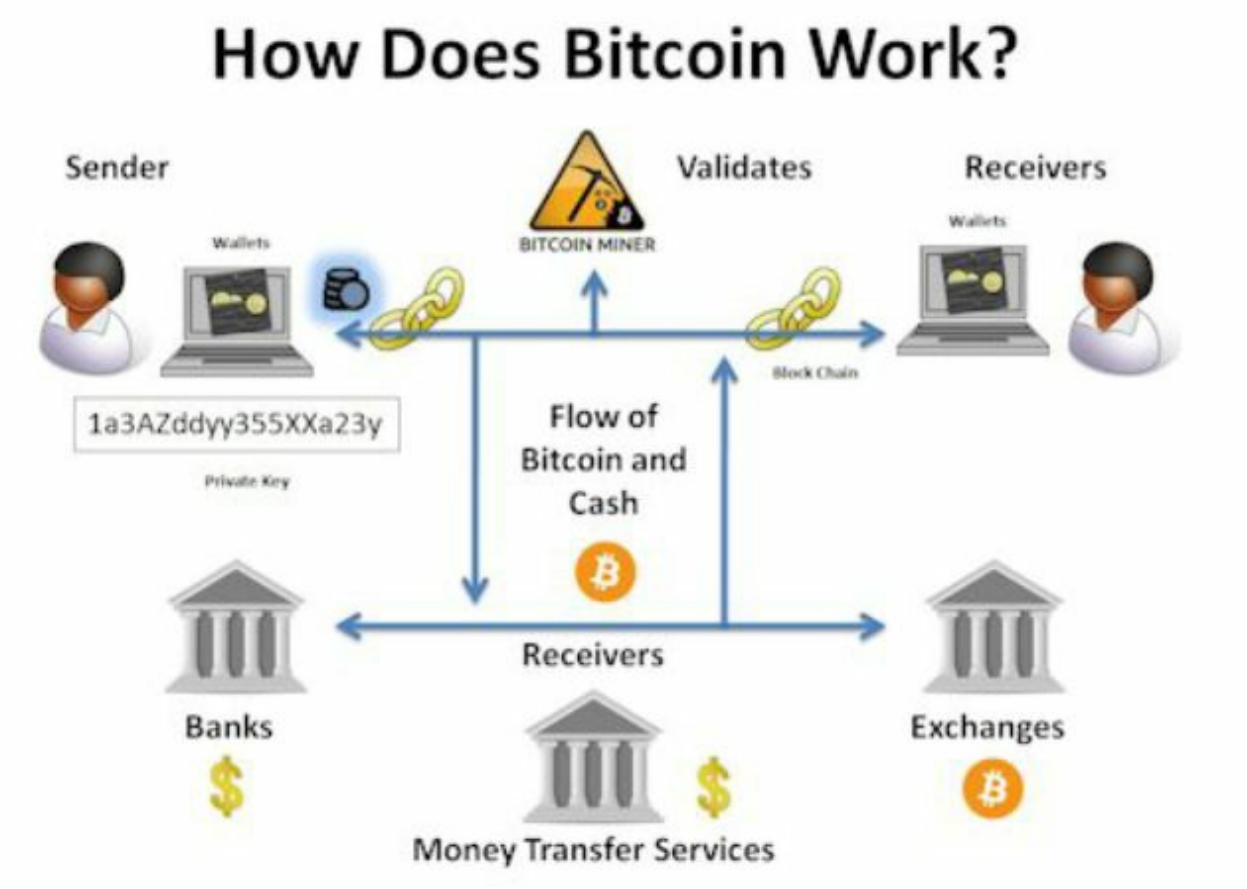
Proof-of-Stake avoids computational waste by requiring the "prover" to show ownership of coin (money). The caveat is that the only types of money

that work with a proof-of-stake system are cryptocurrencies of that same protocol, and thus the technology has only recently become possible**.** **PPCoin** (Peer coin) is using **POS** hash algorithm and ethereum is scheduled to switch from **PoW** to **PoS** in the near future.

Proof of Burn works exactly the way you thought: instead of burning electricity you “burn”your digital coins. No, you do not have to format your hard drive. You "burn" them by sending to such address where they cannot be redeemed! For example, to the address which is a hash of a random number: chances for someone picking public and private keys for it are negligible.

Thus, by throwing away your coins, you get the rights for life-time mining, which is a lottery among the owners of burnt coins.

Proof of Capacity is an implementation of a popular idea of *"megabytes as resources"*. You do not have to burn anything, but you have to allocate significant volume of your hard drive space to start mining. Besides being energy efficient, this approach also provides botnet protection. It is quite hard to install on victim's PC a miner, which would secretly steal a couple of terabytes.



This Diagram explains how a typical Bitcoin or any altcoin works.

The Byzantine Generals' Problem (BGP)

The problem of building a purely distributed but trusted system is not a new one in computer science. It is a common challenge in distributed systems with no central control to enforce trust and, is more generally, a sub-set of the study of fault tolerance. Imagine, for example, a computer system with distributed components that need to communicate information to each other, but that information might fail to communicate accurately (or at all) due to technical failures.

The Byzantine Generals' Problem, first proposed by Marshall Pease, Robert Shostak and Leslie Lamport in 1982, provides a stylized description of this problem;

"We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that (A) All loyal generals decide upon the same plan of action and (B) A small number of traitors cannot cause the loyal generals to adopt a bad plan"
- The Byzantine Generals' Problem, 1982

Bitcoin, however, a system proposed in a white paper released in November 2008 under the pseudonym ***Satoshi Nakamoto***, is the best solution to this problem that has been proposed to date and has had, by far, the broadest adoption.

This problem is called ***Byzantine Fault Tolerance.*** It is stated as follows:

The objective of Byzantine fault tolerance is to be able to defend against Byzantine failures, in which components of a system fail with symptoms that prevent some components of the system from reaching agreement among themselves, where such agreement is needed for the correct operation of the system. Correctly functioning components of a Byzantine fault tolerant system will be able to provide the systems service assuming there are not too many faulty components.

What Does it have to Do with Cryptocurrencies?

Satoshi answers this question.

Using the **Proof-of-Work** mechanism, the generals can solve this problem (which is actually very hard in practice and completely insolvable for two generals!) as they need, in fact, a mechanism for decentralized consensus as a way to find out what the majority thinks and contribute themselves.

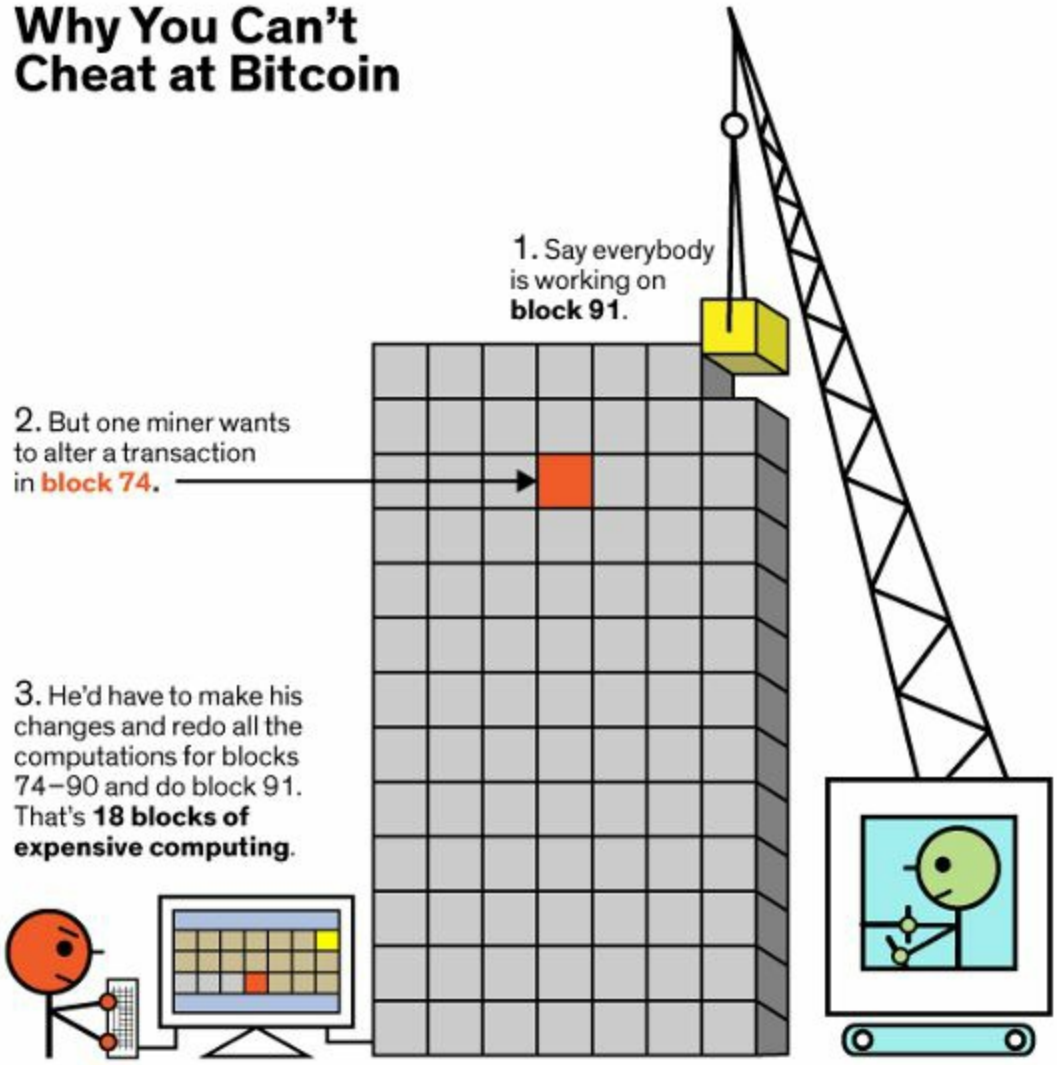
In cryptocurrency, the *generals* are *network nodes*, their messages are a chain of blocks.

The true one is the longest (the one that appeared as a result of more work).

There is an important thing to note though: in Satoshis model we get a random solution (if an attacker has hashrate of x%, he can fool the network with a probability of y%), while the classical problem implies determined algorithm.

Remember we mentioned 51% in an earlier section.

Why You Can't Cheat at Bitcoin



1. Say everybody is working on **block 91**.

2. But one miner wants to alter a transaction in **block 74**.

3. He'd have to make his changes and redo all the computations for blocks 74–90 and do block 91. That's **18 blocks of expensive computing**.

4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

This diagram explains how operations are carried out on a typical Bitcoin Blockchain.

The 51% Attack

51% attack refers to an attack on a blockchain – usually bitcoin network, for which such an attack is still hypothetical – by a group of miners controlling more than 50% of the networks mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users.

They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

They would almost certainly not be able to create new coins or alter old blocks. So a 51% attack would probably not destroy bitcoin or another blockchain-based currency outright, even if it proved highly damaging.

Have you figured how bitcoin solves the Byzantine Generals' Problem?

It is by assuming that ***so long as honest (or, at least, non-collaborating) miners consist of at least 51% of the hashing power in the system, it's trusted. The majority is expected to do the right thing because the protocol was designed to reward those who do honest work.***

So, it is important for the ecosystem of any cryptocurrency blockchain, that honest miners maintain at least 50% of the computational power in the network (alternatively, that no single dishonest miner, or coalition of miners, gains more than 50% of the computational power in the network).

That will greatly violate the integrity of the network.

Top 10 Cryptocurrencies You Should Know.

The total Market Capitalization for all cryptocurrencies as at July 1, 2017 was $109 Billion!

Not all cryptocurrencies are created equal.

Some feature amazing underlying blockchain technology behind its creation. Some were created 'just because', or as a joke. Some were part of an elaborate pyramid scheme. Some are pretty useless to keep as they are perceived as worthless – any cryptocurrency is only as valuable as the value assigned to it by a mass audience.

Like any other assets *(think of stocks, or property)*, its price can rise and fall quickly, making them highly volatile and risky investments.

Here are the top 10 cryptocurrencies and what they are known for.

1. Bitcoin

Price as at 1 July, 2017 $2,600. MKT CAP: $42.7 billion.

The original cryptocurrency and the one that started it all, bitcoin was created and released in 2009 by Satoshi Nakamoto, an anonymous figure. Bitcoin has the biggest market cap to date around $45billion, overshadowing all other cryptocurrencies in this list, combined.

Because Bitcoin has such a big reputation, all other cryptocurrencies are referred to as 'altcoins' – alternative coins because they are alternatives to bitcoin.

Uses SHA-256 PoW hash algorithm.

Known for: *being the first, easiest to get, widest acceptance*

2. Ether

Price as at 1 July, 2017 $310. MKT CAP: $25.1billion

Ether is the cryptocurrency for **Ethereum**, a decentralized platform that can execute peer-to-peer *'smart contacts'*.

As of September 2016 and as a result of an attack to the DAO, Ethereum was split into two: Ethereum (ETH) and Ethereum Classic (ETC). Created by ***Vitalik Buterin*** and launched in mid-2015 after a successful crowd sale, this platform was marketed as the *"next generation cryptocurrency and decentralized application platform"* and has a market cap of $25.1 billion.

Peer-to-peer smart contracts are what Ethereum is known for, aside from the cryptocurrency. It enables people to code and enact contracts without third parties.

Uses ETHASH-256 PoW hash algorithm. Soon to switch to PoS soon.

Known for: *smart contract, first alternative to bitcoin*

3. Litecoin

Price as at 1 July, 2017 $50.00 MKT CAP: $2.41billion

Litecoin was released in October 2011 by former Google and Coinbase employee Charles Lee as an alternative to Bitcoin. Overall, Litecoin is similar (and familiar) – it can be mined, used as currency and transacted for goods and services.

It has a market cap of roughly $2.4billion.

Uses Scrypt PoW hash algorithm.

Known for: *alternative to Bitcoin, most similar to Bitcoin*

4. Monero

Price as at 1 July, 2017 $48. MKT CAP: $665.1million

Bitcoin is frequently mislabeled as an ‘anonymous’ currency (it’s not). Monero, on the other hand, is a cryptocurrency that focuses on privacy – using the ring signature technology, Monero is ‘secure, private and untraceable’.

At fourth place with $665 million in market cap, (at the time of writing) Monero is mostly used by individuals wishing to remain incognito on the web.

Uses Cryptonight hash algorithm.

Known for: *being a privacy-centric cryptocurrency*

5. Ripple

Price as at 1 July, 2017 $0.233 MKT CAP: $9.1billion

The next on the list, Ripple, is actually a real-time gross settlement system, currency exchange and remittance network. The cryptocurrency is called ripples. Released in 2012 and with a current market cap of $9.1 billion, the Ripple system has been integrated into a few banks and payment networks to reduce costs.

Uses SHA-512Half hash algorithm.

Known for: *strong focus on banking market, real-time settlement.*

6. NEM (XEM)

Price as at 1 July, 2017 $0.16 MKT CAP: $1.4billion

NEM is not just a crypto currency. NEM is a blockchain project which caters to much more than only handling it's native currency tokens "XEM". Above that, and more importantly, NEM is a peer to peer platform and it provides services like payments, messaging, asset making, and naming system.

Uses Proof-of-Importance hash algorithm.

Known for: *An encrypted messaging solution that also allows unencrypted and hex messaging*

7. Dash

Price as at 1 July, 2017 $196. MKT CAP: $1.4billion

Dash (short for 'digital cash') is a cryptocurrency with a strong focus on both privacy (using anonymization technology) and speed (of transaction). It was re branded from *Darkcoin* as an attempt to stop being associated with the 'dark web'.

Market cap of $1.4 billion currently rolling out *Dash Evolution*, an attempt to make the cryptocurrency more user-friendly. You can spend Dash several merchants accepting it.

Uses X11 hash algorithm.

Known for: *being anonymous and fast.*

8. MaidSafeCoin

Price as at 1 July, 2017 $0.48 MKT CAP: $205.1million

MaidSafeCoin (also known as Safecoin) is the cryptocurrency for the SAFE (Secure Access for Everyone) network, which is a security-centric data platform. Calling themselves a 'crowd-sourced internet', you can provide space in your computer in exchange for coins.

A number of decentralized apps now use the SAFE network to store data securely. The market cap for MaidSafeCoin is about $205 million.

Uses Proof-of Resource hash algorithm.

Known for: *being a security-centric data platform*

9. Lisk

Price as at 1 July, 2017 $2.33 MKT CAP: $261million

Lisk is a crowd funded cryptocurrency, and a unique one. It brands itself as "the first modular cryptocurrency utilizing sidechains". Unlike other systems on this list (aside from Ethereum), the Lisk system can be used by anyone to make their own decentralized apps ('DApps') in the programming language Javascript.

As such, this currency has practical application value and can be used to create many types of 'DApps', including social media platform, e-commerce store, and many others. It currently has a market cap of around $261 million.

Uses Proof of Stake hash algorithm.

Known for: *useful for programmers to make own 'dapps', the first to utilize sidechains.*

10. Stratis

Price as at 1 July, 2017 $5.23 MKT CAP: $515.1million

Stratis is a simple and affordable end-to-end solution for native C# and Net blockchain applications development. It is developer friendly. The market cap is $515 million.

Uses Proof of Stake hash algorithm.

Known for: *Rapid deployment of Dapps.*

There are over 1,000 cryptocurrencies flying around in the cyber space at the point of this writing. You can always check them out on sites like coincap.io or coincompare.com, or coingecko.com.

A good practice is to read their White Paper, and browse through their forum discussions.

Always do your due diligence before buying any cryptocurrency. Cryptocurrencies with less than $100,000 market capitalization are usually susceptible to internal manipulations. Stay away from those. Avoid centralized digital currencies and currencies that are tied to Pyramid schemes.

They are pure red flags for Ponzi!

Bitcoin in Practice

Bitcoin being the first cryptocurrency to gain mainstream adoption has become the de facto standard for other cryptocurrencies. So most of what we talk about bitcoin here also applies to altcoins.

Some Basic Bitcoin Metrics as at July 1 2017

Price: $2,600

Available supply: 16,434,512

Total Market Capitalization: $42.7 Billion(Total number of issued & available bitcoin X current price).

Total Hash Rate: TH/s **5,002,326.74**

Bitcoin Difficulty: 708,659,466,230

What Makes Bitcoin so Valuable?

Bitcoin derives its unique value from the fact that despite its lack of official backing or government acceptance, it has generated an ecosystem in which many people are willing to trade and accept. In fact, some perceive bitcoin to be more valuable, or more useful, than other currencies in that it is a better option for certain purposes, such as seamless digital transfers and use across borders. Also, because there is a cap set on the total number of bitcoins that will ever exist, the currency cannot be devalued through inflation as others can. Finally, a key benefit of bitcoin is known as “censorship resistance,” its ability to be used for transactions that could normally be censored by other payment networks. Bitcoin has also become a viable store of value.

Bitcoin is more valuable than gold!

Gold Price per Ounce is $1,226.2, while 1 bitcoin sells for $2,600.

Bitcoin out-performed all other forms of investments including real estates in 2015 and 2016!

Bitcoin Wallets

"A wallet is a software that holds all your addresses. Use it to send bitcoins and manage your keys."
(From Antonopoulos, Mastering Bitcoin)

The ***private keys*** that are necessary for accessing a bitcoin address are stored on a **"bitcoin wallet."** In general, wallets grant you access to your ***public bitcoin address*** and allow you to sign off on transactions but, they differ based on how you choose to access them.

Factors to consider when choosing the best bitcoin wallet for you include ***security, anonymity and control.***

Your bitcoin ***private key*** is a randomly generated string (numbers and letters), allowing bitcoins to be spent. A *private* key is always mathematically related to the bitcoin wallet address, but is impossible to reverse engineer thanks to a strong encryption code base.

A wallet address, is an identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3, which represents a possible destination (private key) for a bitcoin payment.

Bitcoin addresses are case-sensitive. Bitcoin addresses should be copied and pasted using the computer's clipboard wherever possible. ***Beware of clipboard malware that have the ability to replace copied addresses with fake ones. To be on a safe side, break the address into to places and copy separately!***

Bitcoin transactions are irrevocable. Once sent, it can never be retrieved back unless the recipient sends them back to you. So double check the address before you hit the send button.

You can share your wallet address which is your public key, but never share or reveal your private key.

He that has a private key owns the coins in it!

The keys within each user 's wallet allow the user to sign transactions, thereby providing cryptographic proof of the ownership of the bitcoins sourced by the transaction.

Keep in mind that if you **don't know who generates your private keys, where they are stored, or if someone else has them** (as when using an exchange site), **they are not actually yours**, as seen in the case of MtGox, which discontinued operations in February 2014.

In February 2014, Mt. Gox suspended trading, closed its website and exchange service and filed for bankruptcy protection from creditors. In April 2014, the company began liquidation proceedings.

Mt. Gox announced that approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time and worth about $2.2 billion today!

Most wallet issuers will ask you to create a password to your account.

That password is not your private key. It is the key to your private key!

Protect both of them with guarded jealousy.

The private key is usually found in such wallets within your personal information section.

A brief on Bitcoin Scaling issues

If you have been hanging out with bitcoin discussants on online blogs, twitter or in meet ups, it is most likely that you will have been hearing phrases like "*Bitcoin fork*" "*Blocksize Increase*" "*Hard Fork*" "*Mining Threshold*" "Bitcoin is dead" "*Bitcoin is about to break*" "SegWit2X" "UASF" etc. All of these phrases are focused on one thing; how do we scale bitcoin to perform better without compromising its foundational principles. I will use this section to briefly help you understand the broad strokes of the discussion, of course without the technical bells and whistles. Perhaps you may wish to dive deeper and do your own research latter.

Background on the Bitcoin Blockchain *(Example purposes).*

- In the Bitcoin protocol, which is a blockchain, these blocks are essentially clumps of transactions that are put together and archived/ confirmed into the network.
- Imagine a typical block being just like an excel spreadsheet tab… With 1000 rows. If you get to 1000 rows, in order to keep recording transactions, you have to open a new tab that has another 1000 rows. This is how it is with new blocks in the blockchain. The blocks are just like the new tabs in the excel file.
- Bitcoin network typically can process 7 transactions per second, because of its 1 MB block size limit.
- Bitcoin network gets more popular every day, so people are now sending more than 7 transactions per second.
- This is causing transactions to get a lot of backlogs when everyone is looking to use the network (whether for practical reasons, or people spamming a lot of meaningless little transactions to fill those rows in the spreadsheet and force others to not get their transaction into a block quickly enough).
- The result is that now, in order to make sure that your transaction does

not get backlogged, you have to increase your *"miners fee"* (Most default to 0.0004 every transaction with bitcoin, which is less than $0.35c).
- This basically is the equivalent of tapping the bitcoin miner on the shoulder (the people who verify your transaction/ essentially delivering to your counter-party) and saying "Hey! If you can let my transaction through before everyone's own, I'll pay you a little bit extra for it."

Increasing the miner's fee means that it is the beginning of the end of the dream of "Sending one billion dollar worth of bitcoin for few cents".

- **Coinbase** (a popular exchange) is no longer paying the miners fee for their customers, because it has gotten too high for them to bear alone so they pass it out to their customers
- **Bitpay** (another well-known exchange) is also no longer paying the miners fees on small transactions because it's not profitable for them to do so.

Hence two main proposals to solve this problem:

Segregated Witness (Bitcoin Core developer group) *a.k.a BIP148.*

It is important to understand that all transactions in bitcoin have two main types of information contained within them:

- One part is the sum of what is transferred from where to where, in the form of inputs and outputs.

- Second part is proof that those transfers are authorized by the respective private key holders and they can be validly confirmed.

This second last part is what is called the "Witness" part.

The basic idea behind **SegWit**, (short for Segregated Witness), is that removing this "witness" from the transaction, enables more transactions to be recorded to the blockchain and thus a higher number of transactions can be

accommodated. Let us take a deeper look at what this means, and what benefits or risks it might introduce into the network.

• More transactions per second since the "witness part" will not be included in the blockchain.

• There will be no "transaction malleability" *(an attack that lets a person change a bitcoin* ***transaction's*** *unique ID before confirmation on the bitcoin network)* for segwit transactions.

• Witness part to be included in "add-on" blocks verified as part of a miners' coinbase transaction. *(A coinbase transaction is the first transaction in a block. Always created by a miner, it includes a single coinbase).*

• The whole value chain within Bitcoin, miners, nodes, wallets, etc will need to be upgraded to gain maximum benefits. Just to mention a few.

Segregated Witness technical details can be found here: *https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki*

Blocksize increase-Bitcoin Unlimited- Bitcoin Cash Group

(Majorly made up of mines and infrastructure owners)—This one doesn't really need too much explanation. It seek effectively the doubling of the size of capacity in the software. (Like in the example at the start, it's like allowing 2000 rows per tab on our spreadsheet instead of 1000). This group is proposing that the blocksize be increased to 2MB or 4MB in other to accommodate more transactions.

Why is this second option a big worry to many people?

- One of the big dreams of Bitcoin is decentralization. If you raise the blocksize to 2MB, you make it harder for people that are not big miners to run a "node" on the network (that's just a way of saying "helping" the network process transactions).
- If it now becomes hard to join a node on the network, we will rely on the big miners to do everything (which they have been doing very well thus far). However, is it putting too much power in the hands of a few large enterprises (big mining companies in China) that could then potentially

abuse this power and control the network?

-

All the big miners in China and around the world benefit a lot more when the blocksize is increased, compared to Segwit solution. So it is an economic issue as well as social issue.

But generally ***SegWit*** seem to have the support of the whole community because most people want the bitcoin network to scale and remain safe. So you might ask why is this so difficult to resolve? The main tension point is between some of the largest miners in China like AntMiner and the expectations from the Core team.

I understand that there was an agreement (NYC Agreement) put in place that SegWit would be accepted if a corresponding increase to the overall block size to 2MB is implemented. This was thought to have been a simple deal to satisfy both the large mining pools and the core team. However as of present there has been no implementation of a bock size increase to 2MB, and on the bitcoin Core website, and there has been talk of SegWit giving the block size a 'theoretical' increase to 4MB due to the amount it has cut down transaction in sizes. As at the time of publishing, this issue had not been resolved but a tentative date of activation was set for August 1, 2017. Will the block size issue be resolved with peaceful agreement between Core and the Miners? Or will people get fed up and start looking towards Bitcoin Unlimited, or give up hope on scaling altogether? Will this $46 billion value economy go up in flames because of scaling disagreements? Your guess is as good as mine.

Currently, people are discussing the next step of the Segwit2x plan after the Segregated Witness protocol is implemented, which is the 2MB hard fork. The hard fork subject remains a contentious topic, and people are wondering if NYA participants will still support the hard fork after Segwit gets implemented. Since the miners are more in number as per running more nodes than developer, they can force a hard fork which could split the network, because both implementations cannot live together on the same network at the same time.

Summary of what we expect

- Under Bitcoin Improvement Proposal (BIP) 148, Bitcoin will be undergoing a user activated soft fork on August 1, 2017.
- Miners *may* hard fork after 12 hours of Segwit.
- There are three possible outcomes of the soft fork, although the exact outcome is unknown as the outcome will depend on the actions of the nodes on the network.
- In a worst case scenario, BIP 148 could cause bitcoin to chain split into two separate blockchains, one with SegWit activated and one without.
- Long term Investors are advised to move their bitcoins from exchanges to personal wallets like hardware wallets or paper wallets.

If you *don't* control your keys during a chain split three main things ***may*** happen:

1. Your bitcoin balance will stay the same and you will be able to use *that* bitcoin token as usual.
2. Your bitcoin balance will be *zero* overnight since your wallet chose the wrong chain.
3. Your wallet provider will offer you a chance to keep your token balance on both chains or to choose one of them.

Be wise and keep your coins off exchanges or from places where you do not have control of your private keys. It is not just because of this expected fork, but as a rule of the thumb!

Types of Cryptocurrency Clients

The terms Bitcoin "*wallet*" and "*client*" are sometimes used interchangeably. But let me distinguish wallets and clients as follows:

• A **wallet** is a **collection of data** (e.g. the bitcoin user's private/public key-pair and his address) enabling a user to receive and send bitcoins, in the form of spendable outputs.

• A **client** is the **software** that connects a user to the bitcoin network. It handles all the communication, updates the wallet with incoming funds and uses information from the wallet to sign outgoing transactions.

With this understanding in mind, lets us look at the different types of bitcoin clients:

• **A Full client**, or *"full node"* is a client that stores the entire history of Bitcoin transactions, manages the user's wallets and can initiate transactions directly on the bitcoin network. This is similar to a tandalone email server, in that it handles all aspects of the protocol without relying on any other servers or third-party services. In full clients, the private keys ***are never communicated and are stored locally.***

• **A Web client** is accessed through a web browser and stores the user's wallet on a server owned by a third-party. This is similar to webmail, in that it relies entirely on a third-party server. Some web clients are just an interface with the service's servers (e.g. coinbase) where the private keys are stored, and others (e.g. Blockchain.info, greenaddress.io) also store the users' private keys encrypted, but only the user can decrypt them locally on his computer.

A Lightweight client stores the user's wallet but relies on third-party owned servers for access to the bitcoin transactions and network. The lightweight client does not store a full copy of all transactions and therefore must trust the third-party servers for transaction validation. This is similar to a standalone email client that connects to a mail server for access to a mailbox, in that it relies on a third party for interactions with the network. Lightweight clients store private keys locally, just like full clients.

• **A Mobile client**, usually used on smartphones, can either operate as a full client, a lightweight client or a web client. Some mobile clients are synchronized with a web or desktop client, providing a multi-platform wallet across multiple devices, with a common source of funds.

Paper wallets: These are fashioned wallets, where the bitcoins are stored on papers. They hold the bitcoins in an offline mode so that they are highly safe. They provide control over the private keys used. They cannot be recovered as hardware wallets. There is a chance for the loss of bitcoins due to the fade or destruction of papers.

A **hardware wallet** is a special type of bitcoin wallet which stores the user's private keys in a secure hardware device. These are a type of physical wallets are recommended for the storage of a considerable amount of bitcoins. They are portable with user-friendly nature. They control bitcoins with the help of plug and play options.

They have major advantages over standard software wallets:

- Private keys are often stored in a protected area of a microcontroller and cannot be transferred out of the device in plain text.
- Immune to computer viruses that steal from software wallets.
- Can be used securely and interactively, as opposed to a paper wallet which must be imported to software at some point.
- Much of the time, the software is open source, allowing a user to validate the entire operation of the device.

A "Key" Choice

Having your keys stored locally or remotely (i.e. on a third-party's server) is a question that depends on your Bitcoin wallet and client choice. Bear in mind that, the security of your funds also heavily depends on this choice, thus your decision must be made carefully. Below, we examine some of the pros and cons of storing your wallet locally or remotely.

Locally: If your computer is compromised by a hacker, if it crashes (and you have no backups) or if you forget your passwords, your private keys (and bitcoins) will most probably be lost forever! However, if you take reasonable steps to avoid intrusion or exposure, your keys will be reasonably safe and protected from third-party failure or intent. In this case, you exchange convenience for **increased** security.

Remotely: If the third-party exchange's security is compromised, or if they act maliciously, your bitcoins will most probably be lost forever! Bitcoin exchanges are **not** Banks. Most will provide a method of changing your passwords if you forget them, and employ security experts and suitable infrastructure, so you will not have to worry about taking extensive security measures. However, third-party exchanges are more likely targets for intruders and, if compromised, they could steal your bitcoins. In this case you exchange security for **increased** convenience.

It is important to note that most of the security vulnerabilities reported on bitcoin holdings are usually on the user wallets or exchange levels. The security of the bitcoin network remains top notch and unbreakable.

You should always do research before downloading or installing any Bitcoin wallet. Many wallets are malware and will just steal your bitcoins once you fund the wallet.

All wallets that are directly connected to the internet are known as hot storage wallets. The ones that are taken offline and only reconnected or reloaded as when needed are known as cold storage wallets.

Best hardware wallets for Bitcoin.

If you want to store bitcoin other cryptocurrency securely for long term, then you should definitely order a hardware wallet. As at the time of this

writing, there has been no reported theft or loss of bitcoins from a hardware wallet. Some hardware wallets have security grid cards, and some have a little digital screen with a user interface to verify transactions. Even in the case of damage to your hardware wallet, you can restore your bitcoins easily with the recovery phrase.

Ledger Nano S

Some of its core features are the backup seed key for recovery of your bitcoins, the ease to use OLED interface, and a flash drive like feel, with two buttons on the side for navigating the interface. It is a battery-less device which you can connect to a PC or mobile device via USB.

Trezor

It looks like a small calculator with an OLED screen. Randomly generated nine digit pins and a 24-word recovery seed key ensures security in case the device is lost or damaged. Its purpose is to store private keys and sign transactions offline. Trezor now supports eight cryptocurrencies including Bitcoin.

KeepKey

It has same backup seed key feature with pin code enabled, and it works like the other wallets. At present, it supports six cryptocurrencies (including Bitcoins).

There are, of course, some other hardware wallets out there; but these three stand head and shoulder above the rest, from my opinion.

USB thumb drives can also serve as hardware wallets.

Sending and Receiving bitcoins.

There are various ways for you to get your first bitcoins:

• **Offer a Service or Product for bitcoins**. There are many ways you can go about this and many businesses and individuals already accept bitcoins.

• **Accept bitcoins as a donation,** e.g. if you are running a charity.

• **Purchase bitcoins through an Exchange,** e.g. to get relatively large amounts of bitcoins at the current market price.

A very comprehensive list of bitcoin exchanges, categorized by country, can be found at ***http://howtobuybitcoin.info.***

Identity verification will typically be required before you can buy/ sell bitcoins and deposit/ withdraw fiat currencies. Thus, it might take some time.

Another way of getting bitcoins is through faucets.

When first created, a bitcoin wallet is empty.

In order to receive some bitcoins, we have to inform the sender about your wallet's bitcoin address, just like we would provide our email address to someone who wants to send us an email. To send bitcoins e.g. when using a desktop client, you can just copy this my wallet address and paste it into receivers address field:

1NfG7Vhkaz97EYUk JQCwjMRzFKfRxeLf7K

If the sender is using a mobile client, it could be more convenient to scan the QR code above.

Get the real feeling, send a few mBits (1/1000 BTC) to my wallet https://chuta.bitcoinwallet.com/

How Digital Currency transactions work on The Blockchain

Bitcoin transactions are sent from and to electronic bitcoin wallets, and are digitally signed for security. Everyone on the network knows about a transaction, and the history of a transaction can be traced back to the point where the bitcoins were produced.

Holding onto bitcoins is great if you're a speculator waiting for the price to go up, but the whole point of this currency is to spend it, right? So, when spending bitcoins, how do transactions work?

There are no bitcoins, only records of bitcoin transactions.

Here's the funny thing about bitcoins: they don't exist anywhere, even on a hard drive. We talk about someone having bitcoins, but when you look at a particular bitcoin address, there are no digital bitcoins held in it; in the same

way that you might hold naira or dollars in a bank account. You cannot point to a physical object, or even a digital file, and say “this is a bitcoin”.

Instead, there are only records of transactions between different addresses, with balances that increase and decrease. Every transaction that ever took place is stored on the block chain. If you want to work out the balance of any bitcoin address, the information isn’t held at that address; you must reconstruct it by looking at the blockchain through its block explorer.

What does a transaction look like?

Basic transactions have three pieces of information:

- An input: This is a record of which bitcoin address was used to send the bitcoins i
- An amount: This is the amount of bitcoins that was sent.
- An output: This is receiver’s bitcoin address.

Why must I, sometimes, wait for my transaction to clear?

Because your transaction must be verified by miners, you are sometimes forced to wait until they have finished mining. The bitcoin protocol is set so that each block takes roughly 10 minutes to mine.

Some merchants may make you wait until this block has been confirmed, meaning that you may have to make a cup of coffee and come back again in a short while before you can download the digital goods or take advantage of the paid service.

On the other hand, some merchants won’t make you wait until the transaction has been confirmed. They effectively take a chance on you, assuming that you won’t try and spend the same bitcoins somewhere else before the transaction confirms. This often happens for low value transactions, where the risk of fraud is not as much.

Are there any transaction fees?

Well, Sometimes …every time.

Transaction fees are calculated using various factors. Some wallets let you set transaction fees manually. Any portion of a transaction that is not picked up by the recipient or returned as change is considered a fee. This then goes to the miner lucky enough to solve the transaction block as an extra reward.

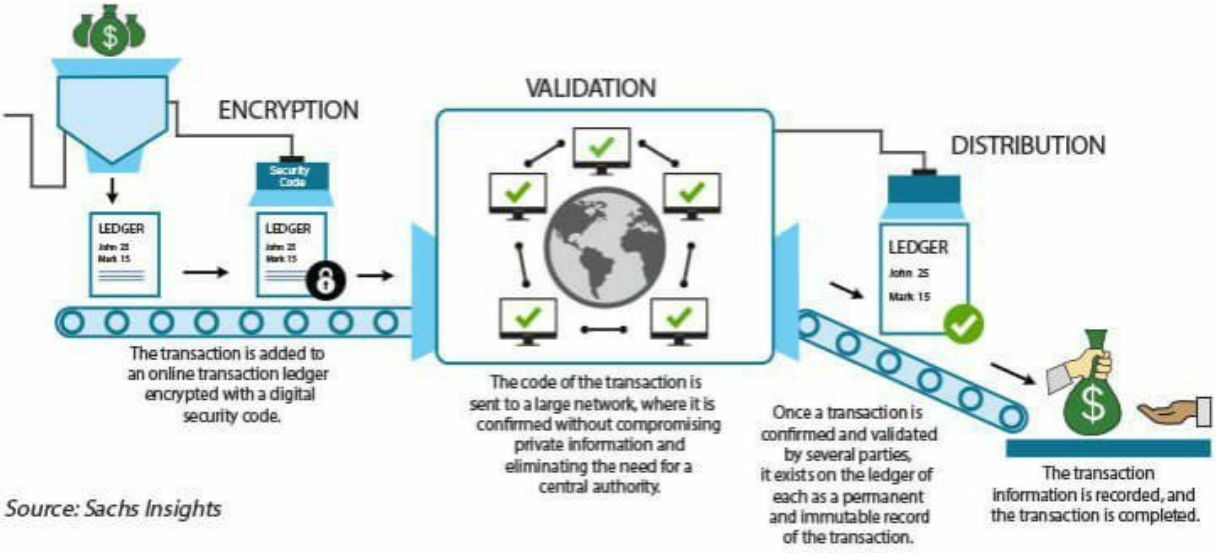
If you will like to know how much your transaction fee will be use this website; http://bitcoinfees.21.co/

If you are wondering about how many nodes are currently mining on a bitcoin network, https://bitnodes.21.co/

At the time of writing, the global bitcoin nodes distribution, i.e. reachable nodes as of Fri Jul 14 2017 20:05:26 gmt+0100 (W. Central Africa standard time) was **7973 nodes**.

Anatomy of a Typical Blockchain Transaction

Here's a step-by-step breakdown of how a transaction between two parties occurs algorithmically via distributed ledger technology.



Source: Sachs Insights

Possible Frustrations when you Ignore Important Security Warnings in this book.

- When things turn sore in an attempt to generate a license key for some extremely desirable game or licensed software. This software will scan your hard disk, then it will find your private key. After a few milliseconds a new transaction appears on the bitcoin network that will take all of your hard-earned money.
-
- If your *c-panel email* provider claims that it has lost the database of its users. Then some guy "Joe" will buy it in the "darknet", "deep web" and quickly begin to run different semantic analyzers. After a couple of hours, it will lead to the disappearance of all bitcoins from all of the services that use authorization via email, after a couple of hours.

- In another case, some guy "Peter", who works for Google and has admin rights (like Snowden had) simply steal your bitcoins from some service. And nobody will notice that. It will be like magic.

- Some virtual exchange, where all of your cryptocurrency is stored will disappear along with all the money. Exactly what Mt.Gox did and dozens of others.

- If you catch some trojan in the process of hunting for a cool porn. It can

encrypt all the files on the hard disk. Afterwards it will find all links to your wallets and it quickly realize how much money you have and how much money it can demand from you. If you won't pay, your hard drive will not be decrypted. Remember the ramsomeware attacks? This is a tragic scenario. After all, you can't even send money to this hacker, because your keys are still on the encrypted hard drive!

- If you lose your unencrypted laptop or phone.

- If you catch a clever Keylogger, none of your activities will save you from epic fail.

- If you get an email from the service where your crypto-money is stored. However, the name of website is not blockchain.info but, for example, blokchain.info, or for "coinbase.com" you see "cainbase.com" and all will look identical. If you click on the link and successfully authorise it, simultaneously your bitcoins will disappear.

- One morning you will wake up without your money because the NSA agent will take advantage of some delicious backdoor in your Windows operating system.

- If you decide to transfer cash to the Smart Contract that you think will do what it said it will do on its ICOs white paper to do, and turns out to do something else. The *smart contract* turns out to be smarter than you are and scams you.

Clearly, this is not a complete list. But, maybe, it will give you some ideas when something goes wrong. Now you see, cryptocurrencies—is not all about making big money. Its risk prone. You are fully responsible for the safety of your coins. Neither Jesus Christ nor the Pope, nor Vladimir Putin nor Donald Trump will be able to help you if you do something wrong, or leave undone those things you ought to have done to secure your fund. But the bad guys can't take your money if you do everything you ought to do in the right way, and on time too!

Enough said!

Securing your Hard Earned Cryptowealth.

As stated elsewhere, cutting out the middlemen, banks, traders, card issuers etc is great but that comes with its own huge responsibility as you must have basic understanding on how to protect ourselves as you have becoming a one-man financial institution. No SEC, No Insurance. No Central Bank. You are now on your own. It is therefore very important you take some serious security measures to secure your financial future. While the protocols underlying bitcoin and most cryptocurrencies have proved themselves to work well and secure, the weak links have been the software containing the wallets, whether on exchanges or on individuals' computers. With great power comes great responsibility. My overall recommendation is to increase your computer literacy.

So, how can you protect yourself?

Bearing in mind that you need to protect both your identity and your wallets from potential digital theft note this: *Do not give ANYONE your private key!*

Use a versatile Bitcoin client

For the purpose of privacy, and to hide your IP address, you can use a Bitcoin client that allows you to change to a new address with each transaction.

Similarly, you can separate transactions into different wallets, according to their importance: a recommended practice is to keep a wallet for day-to-day transactions of small amounts, to be topped up when necessary.

Protect your identity

It is also important to be careful when sharing information about your transactions in public spaces like the web, either voluntarily or unwittingly, so as to avoid revealing your identity together with your bitcoin address.

Use an *"escrow service"*

When you need to buy or sell something and you are not sure who is on the other side, you can use an "escrow service." In these cases, the person who needs to make the payment sends their *bitcoins* to the escrow service while they wait to receive the item they are buying.

Meanwhile, the seller knows their money is safe with the escrow service and sends the agreed item. When the buyer receives the merchandise, they notify the escrow service to finalize the payment. Never do a transaction with someone you don't know very well without an escrow service.

Make a *backup* of your virtual wallet

With regard to physical storage, as with any critically important *backup* policy, it is recommended to make frequent updates, use different media and locations, and keep them encrypted.

Encrypt your wallet

Encrypting your wallet is crucial, especially when it is stored online. As you might expect, the use of a strong password is equally essential. With this in

mind, you can use tools like DESlock+ to encrypt files that contain any sensitive information. I used the Enpass password generator to generate strong passwords and I use encrypted email service from protonmail.com and I like it. Even better is to encrypt the entire system or user space where these files are located.

Don't forget about two factor authentication

When using *online* storage services, it is important to undertake an extensive selection process to determine which are truly reliable. Even then, you have to bear in mind that any provider could end up being subject to the discovery of vulnerabilities in its systems.

As such, it is recommended to use two factor authentication and whenever possible, *online* services that support the use of hardware wallets.

Avoid using wallets on mobile devices

You should avoid using mobile devices, especially in the case of large sums of money, as they can be lost and/or compromised. In these cases, it is actually better to keep the wallet on equipment that is not connected to the Internet.

Consider using multi-signature addresses

For corporate transactions or any transaction that require a high level of security, it is possible to use multi-signature addresses, which involve the use of more than one key, the keys usually being stored on separate equipment in the possession of the authorized staff.

This way, an attacker will need to compromise all the equipment on which the keys are stored in order to be able to steal the *bitcoins*, making their task more difficult.

Update your systems regularly

Naturally, any application can have faults, so it is essential to constantly update your bitcoin clients and your operating system, as well as other products that run on it. Virtual wallets can be affected by any kind of *malware* that might be hosted on the hardware, so it is recommended to have a properly updated security solution to run full scans on a regular basis. I recently lost a large amount of bitcoin due to clipboard malware that replaces copied bitcoin addresses. That was when I learnt to always double check any bitcoin address I want to send coins to.

Get rid of a virtual wallet if you are not using it

Lastly, getting rid of a virtual wallet when it is no longer needed requires a careful process to check that it has really been completely destroyed. On Linux systems, you can use the *shred* command for this purpose, which overwrites the wallet file with random data before deleting it.

It is important to make the effort to locate any copies that might have been created, either by a user or by the system, and then carry out this same process. This is more important if you intend to sell off the laptop.

Now you know how to protect yourself…

Although it is impossible to guarantee total protection of our assets from digital theft, this shouldn't stop us from enjoying the use of the technology.

So long as we make sure to take the necessary precautions, there's no reason not to take advantage of the benefits offered by cryptocurrencies as they make inroads into our economy

Why is Bitcoin and Digital Currencies Booming?

A prime reason why bitcoin and digital currency revolution continues to succeed is the distrust many citizens have in their respective government's currency. They want to use bitcoin as a hedge or an alternative mechanism of payment and transfer when government currency doesn't efficiently perform such basic functions. It's no surprise that millennials, many of whom understand the digital currency much better than their old school forbears, are investing in bitcoin at far greater rates.

All modern fiat currencies depend on trust in a government for their value and stability. Some governments have institutions, like the U.S. Federal Reserve, or Nigeria CBN, that inspire substantial trust, but others have monetarily oppressive regimes many citizens want to bypass. Argentina continually debased its currency until last year. China puts burdensome restrictions on transferring its currency out of the country. Both countries have seen substantial trading in their respective bitcoin exchanges.

Unlike national currencies, bitcoin does not depend on a regime that can be corrupted by politics. With bitcoin, trust is required, but not in government but in the decentralized order of those who verify bitcoin transactions—the miners. They maintain the public ledger on the internet of all bitcoin transactions, which accounts for the ownership of every bitcoin in existence.

Bitcoin's creation of order without centralized law is not unknown to society. Social norms often regulate behavior without the benefit of formal law. Rules of etiquette tell people how to behave at the table without causing offense. But ,while order without law is possible without software, software can improve its enforcement. One might ignore a social convention, but it is impossible to ignore the operation of an algorithm that tells the world whether you own a bitcoin.

To continue to flourish, bitcoin does not have to become a more stable store of value than the U.S. dollar. It can climb the rungs of respectability by prevailing over less trustworthy currencies. It is already gaining strength and stability by competing successfully against monetarily oppressive regimes and helping poor immigrants in the developed world remit money to their relatives back home. As bitcoin gains stability, it can become even more competitive because even the best fiat money is subject to political risks.

National and international crises will continue to fuel bitcoin's rise.

Bitcoin continue to succeed as long as the value of other currencies rests on politics.

Cryptoeconomics and the Internet of Value

What is Cryptoeconomics?

Cryptoeconomics is a discipline that studies protocols that govern the production, distribution and consumption of digital goods and services in a decentralized digital economy. -Vlad Zamfir (Ethereum core developer).

Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols. It is the study of economic interaction in adversarial environments. Cryptoeconomic approaches combine cryptography and economics to create robust decentralized P2P networks that thrive over time despite adversaries attempting to disrupt the network. In simple terms, cryptoeconomics is a new field of study that analyses economic interactions in the decentralized digital economy that was pioneered by bitcoin. It is the foundation on which cryptocurrencies and digital assets are built upon. At the heart of Cryptoeconomics lies economic incentives for all participants.

Typically, cryptoeconomics are used to replace trust in the situations where trust no longer scales, and in hostile environments where everyone wants to take undue advantage of others.

Satoshi Nakamoto birthed the field of cryptoeconomics when he created Bitcoin in 2009. Just like Galileo is known as the founding father of physics, Satoshi will forever be known as the founding father of cryptoeconomics.

Earlier decentralized systems like Kazaa and Bittorrent lacked baked-in economic incentives and this is arguably what stifled these early P2P systems from persisting and thriving over time. Satoshi's combination of crypto and

economic incentives resulted in a robust, thriving p2p payment network that today stores over $100B worth of value and processes over $600M worth of transactions daily.

The point of all these is that anyone anywhere in the world can benefit massively from this economic incentive systems. By plugging in, you become a player and a stake holder in the digital economy. This is how Cryptocurrency mining businesses has become major economic blocks. Don't just stand by and watch, get involved right away. New opportunities spring up on daily basis, no need to bemoan not getting into bitcoin or ethereum earlier.

What is the Internet of Value?

With the Internet of information, we have to rely on powerful intermediaries to establish trust. Banks, governments, and even social media companies like Facebook work to establish our identity and ownership of assets. They help us transfer value and settle transactions.

Overall, they do a nice job -- with limitations. They use centralized servers, which can be, and has been hacked from time to time. They take a fee for their services – say 10 percent to send money internationally. They capture our data, not just preventing us from monetizing it, but often undermining our privacy. They are sometimes unreliable and often slow. They exclude two billion people who don't have enough money to justify a bank account. In sum, they capture a lopsided share of the benefits of the digital economy.

This is the excitement around the blockchain, the first native digital medium for peer to peer value exchange. Its protocol establishes the rules—in the form of globally distributed computations and heavy duty encryption—that ensure the integrity of the data traded among billions of devices without going through a trusted third party. Trust is hard-coded into the platform. That's why we call it the Trust Protocol. It acts as a ledger of accounts, a database, a notary, a sentry, and clearing house, all by consensus.

So the Internet of Value will remove the need for intermediaries in banking, insurance, housing, media, and all sorts of other industries. It will eliminate financial exclusion and make us free by handing control of our identity and our resources back to ourselves. It will provide true democracy and a new kind of truly decentralized organization. It is one of the biggest technological revolutions in our lifetime

With the debut of Internet of Value, a value transaction such as a foreign currency payment, can happen instantly, in the same way people have been sharing words, images and videos online for decades. And it's not just money. The Internet of Value will enable the exchange of any asset that is of value to someone, including stocks, votes, frequent flyer points, securities, intellectual property, music, scientific discoveries, and more.

The Internet of Value is a new kind of Internet where it's possible to exchange value in the form of crypto currencies, contracts, stocks, shares, intellectual property and ownership of valuable things in general.

The Internet of Value is a powerful initiative because it promises a future where everyone has access to free disinter-mediated universal transfers of value. Intermediaries add cost and time to transaction processing.

Public-key cryptography is the most basic enabler of the IoV.

In summary:

- The Internet of Value will lead a fairer, disinter-mediated society.
- The technology underpinning this revolution is revolutionary because it allows adversarial nodes to cooperate as opposed to Internet previous collaborative environments.
- We're still at the beginning and the technology can't still be applied massively.

One project that is of great interest in making the IoV realizable in the nearest future is **the Basic Authentication Token** an ethereum project targeting publishers, advertisers and user. They have identified ***broken system with eroded revenue, trust, privacy*** and they are now proposing a solution through the combination of their pilot project, Brave browser, and BAT to ensure ***Fairness, anonymity, and impact using proven blockchain technology.***

Visit the website to learn more: https://basicattentiontoken.org/

Blockchain enables value exchange

Until now, selling, buying or exchanging these assets has required an intermediary like a bank, marketplace (physical or digital), and credit card Company, or third-party booking services. Blockchain technology, including Ripple's Interledger solution, allows assets to be transferred from one party directly to another, with no middleman. The transfer is validated, permanent, and completed instantly.

About Interlegder

Interledger is an open suite of protocols for connecting ledgers ***(includes IBM Hyperledger)*** of all types: from digital wallets and national payment systems to blockchains and beyond. This technology makes it easy to transact with anyone, no matter where they live or what type of money they use. Sending value becomes as easy as sending information is today. This is the vision of the Internet of Value.

How Interledger Works

On its most basic level, Interledger uses *connectors* to route payments across different ledgers. Conditional transfers -- using Hash-Time-Locked Contracts (HTLCs), as they are known in the blockchain space -- are used to secure multi-hop payments so funds cannot be lost or stolen in flight. On top of this security primitive, Interledger provides a packet and address format, heavily

inspired by the Internet Protocol (IP), to instruct connectors where to forward payments. For more details, visit this website: https://interledger.org/rfcs/0001-interledger-architecture/

World Wide Web 2.0 vs World Wide Web 3.0

Advancements in different technologies are gradually paving the way for a new kind of web.

Web 1.0.

This was the "readable" phrase of the World Wide Web with flat data. Its earliest stages didn't even have GUI. Tools like CuteFTP *(originally developed by Russian programmer Alex Kunadze)* were used in calling web pages over dial up connections. In Web 1.0, there was limited interaction between sites and web users. Web 1.0 was simply an information portal where users passively receive information without being given the opportunity to post reviews, comments, and feedback. I started building websites during this era and I remember how we struggled with dynamic contents. To make any changes, you literally had to take down the entire web-page

Web 2.0.

It is the "writable" phrase of the World Wide Web with interactive data. Unlike Web 1.0, Web 2.0 facilitates interaction between web users and sites, so it allows users to interact more freely with each other. Web 2.0 encourages participation, collaboration, and information sharing. Examples of Web 2.0 applications are YouTube, Wiki, Flickr, Facebook, Twitter and so on. Web 2.0 includes the emergence of the mobile Internet and mobile devices (including camera phones) as a major new platform driving the adoption and growth of the Web. But we also saw a web 2.0 that encouraged data centralization and rise of the internet whales who made fortunes off user generated content and data.

Web 3.0.

This is the "executable" phrase of Word Wide Web with dynamic applications, interactive services, and "machine-to-machine" interaction. Web 3.0 is a semantic web which refers to the future. In Web 3.0, computers can interpret information like humans and intelligently generate and distribute useful content tailored to the needs of users. One example of Web 3.0 is Tivo, a digital video recorder. Its recording program can search the web and read what it finds to you based on your preferences.

A Tel-Aviv based decentralized tech stack Development Company, Synereo has announced that it will be releasing the Alpha phase of decentralized social network in September 2017. A networks that hopes to start chipping away at services like Facebook.

In general, web 3.0 will be characterized by the following;

Ubiquitous Connectivity

- Broadband adoption
- Mobile Internet access
- Mobile devices
- Network Computing
- Software-as-a-service business models
- Web services interoperability
- Distributed computing (P2P, grid computing, blockchains, hosted "cloud computing" server farms such as Amazon S3).
-

Open Technologies

- Open APIs and protocols
- Open data formats
- Open-source software platforms
- Open data (Creative Commons, Open Data License, etc.)
-

Open Identity

- Open identity (OpenID)
- Open reputation
- Portable identity and personal data (for example, the ability to port your user account and search history from one service to another)

The Intelligent Web

- Semantic Web technologies (RDF, OWL, SWRL, SPARQL, Semantic application platforms, and statement-based datastores such as triplestores, tuplestores and associative databases)
- Distributed databases — or what I call "The World Wide Database" (wide-area distributed database interoperability enabled by Semantic Web technologies)
- Intelligent applications (natural language processing, machine learning, machine reasoning, autonomous agents)
-

I see most of the opportunities of the blockchain technology scattered around the unveiling world of web 3.0.

What are you going to do?

Will you just watch or take advantage of the opportunities offered?

Will Criminals Use Bitcoin and Digital Currencies?

The biggest fear among most people concerning the use of cryptocurrencies centers on its regulation status. To them, the fact that these cryptocurrencies are essentially unregulated means there are few reporting and tracking mechanisms in place. They conclude that since suspicious transactions cannot be monitored, are border-less, international, anonymous, and no one has duty to report strange activity to the Financial Intelligence Monitoring Bodies, the risk of vulnerability for financial terrorism remains high. The sector, they say, is currently not organized well enough to receive guidance or relevant information on AML/CFT requirements. They argue that the level of anonymity of virtual currencies provides a modicum of risk, because it plays into the hands of terror cells and other nefarious organizations. In other words, people with violent intentions can use these currencies in a secretive way to fund bombing campaigns or other violent activities.

These are genuine concerns which are too big to be ignored, too small to worry about, and yet moving too fast for it to react or reset. This is a clear dilemma staring at Fintech regulators, because this thing is not going away anytime soon. The blockchain is trustworthy, because it is transparent, crowd sourced and permissionless. Individual users are not directly identified, but the movement of money from one wallet to another can be tracked throughout history by anyone.

And so, transparency is inherent to the network. But, surprisingly, obfuscation can be added as a layered option, and it is fairly easy. I have already dealt with transaction obfuscation in the section on Deep Web.

Let me focus on regulation now.

Regulators need not worry much because bitcoin was created with some properties different from other fiat money widely used. bitcoin is a tool, like a knife, use it to cut your food, or stab someone and your culpability can be established. The paradox of cryptocurrency is that its associated data creates a forensic trail that can suddenly make someone's entire financial history public information. Most of the experts who helped to create the encryption and software systems that made cryptocurrencies possible are now helping law enforcement agencies nab criminals. These experts operate in a new field at the crossroads of computer science, economics, and forensics. So no one needs to panic. Investigators can follow the money!

As criminals have evolved more sophisticated methods to use cryptocurrencies, researchers have followed apace, nay bumper to bumper. All cryptocurrency users are connected in a peer-to-peer network over the Internet. Data flow between their computers like gossip in a crowd, spreading quickly and redundantly until everyone has the information—with no one but the originator knowing who spoke first. The beauty of bitcoin, from a detective's point of view, is that the blockchain records everything. If you catch a dealer with drugs and cash on the street, you have caught them committing one crime. But if you catch people using something like "Silk Road" of the *Deep & Dark Web*, you have uncovered their whole criminal history. It's like discovering their books.

What regulatory and monitoring agencies need is to ensure that a strong Know Your Customers (KYC) and Anti-Money Laundering (AML) and Anti-Terrorism policies are in place at the cryptocurrency exchange level. That is the primary entry point for most cryptocurrency users. Yes, it is possible to get digital currencies from some other sophisticated means, but the exchange is the most plausible avenue that most user start with.

A smart person may ask, what if non-state actors, including terrorist and insurgent groups, seek to increase their political and/ or economic power by deploying their own Cryptocurrency as a medium for regular economic

transactions as opposed to exploiting already-deployed virtual currencies, such as Bitcoin, as a means of illicit transfer, fundraising, or money laundering. After all it does not cost much to lunch a digital currency. Will this not threaten National Security?

OK, the simple fact remains that it would be extremely difficult for a non-state actor to structurally design a cryptocurrency from scratch that would be both resilient to attack and usable by all persons in the non-state actor's geographic area of influence. Such difficulty is especially exacerbated in less technologically sophisticated regions and in areas with incomplete networking infrastructures.

Virtual Currencies are vulnerable to attacks of varying degrees of sophistication.

- Relatively unsophisticated attacks by governments, other non-state actors, or even users of another crypto currency could involve distributed denial-of-service attacks against more centralized services, such as mining pools or online-wallet applications, or attempts to gain control of a Virtual Currency via

exploiting a crypto currency market rules, e.g., by supplying a majority of the computing power for bitcoin-like crypto currency.

- A more sophisticated attacker could conduct zero-day exploits—attacks that take advantage of a software vulnerability that the developer is unaware of and for which no patch exists. Zero-day attacks could target crypto currency services, such as exchanges and wallets, as well as cell-phone applications used for common transactions.

-The most sophisticated challengers could attack the underlying cryptocurrency infrastructure, including hardware, or covertly corrupt the software used by cryptocurrency participants, including through the subversion of the underlying security mechanisms on which the software relies.

I promised at the beginning that this guide will be a non-technical document, so let's consider the details of this sections as being outside the scope of this book. Perhaps in another technical volume, we shall do justice to the subject matter.

Where is Cryptocurrency adoption in the Market Cycle?

Considering everything we have discussed so far about Blockchain and Digital currencies, we are nowhere near ***euphoria*** according to the traditional market cycle. With that in mind, I believe, considering all crypto currencies

combined, whose market capitalization stands at $103Billion, we are only in the ***optimism*** stage in the market cycle and gradually shifting toward excitement stage.

Bitcoin is the only cryptocurrency that has certainly gone through this cycle, reaching *euphoria* in January of 2014. I will not call its hitting $3,000 mark in May 2017 as a *euphoria* stage.

According to ***CoinDesk State of Blockchain Q1 2017*** study, which details recent trends, statistics and sentiment around cryptocurrencies and blockchain technology, the following was reported;

All Cryptocurrencies rally in price

- Nearly the entire Digital asset class rallied in the first quarter as the overall market cap gained $7bn to an all-time high of $25bn. In the months since the end of Q1, the collective market cap of cryptocurrencies has rallied north of $90bn towards $103bn late in May.

Despite bitcoins 10% price gain, its market dominance hit an all-time low as smaller assets made significant gains.

Transactions and fees rise, prompting scaling focus

The first quarter set the record for the most bitcoin transactions per day (287,098), the largest blocks (0.92 MB) and the most expensive transactions ($0.62). In June, transaction fees rose to over $5 .

Other major public blockchains experienced increased usage in the first quarter as well, including ethereum and dash, monero and zcash – a growing sector of privacy focused cryptocurrencies.

Regulators significantly impact global markets

The composition of trading shifted in the first quarter as agencies around the globe made decisions impacting cryptocurrency trading structures and treatment. China is a case in point here.

Interest in permissioned blockchains and enterprise developments increases.

As more traditional companies have become involved in blockchain, they

have added to the research going into the **growing permissioned side of the blockchain space**.

In that time, the Linux Foundation-led Hyperledger project has grown its list of members, proofs-of-concept and frameworks and tools.

DApp tokens and ICOs flourish within small groups

Decentralized applications (DApps) and token sales continue to draw investor interest as short-term returns have been astronomical for many.

Ethereum DApps are not alone in grouping around use cases, as other broad sectors have only become more apparent over time, like privacy-focused cryptocurrencies, DApp platforms, interoperability-based protocols (like Cosmos and Polkadot) and storage-based assets (like Sia and Storj).

Ethereum sentiment far outweighs bitcoin.

The main Spotlight Study in the Q1 2017 State of Blockchain was the *Bitcoin and Ethereum Sentiment Survey.*

The survey revealed that the community was extremely enthusiastic about most aspects around the *state of ethereum.*

That said, a number were torn – and bordering on the negative – regarding many aspects of the state of bitcoin.

Why you should Invest in Digital Currencies and where you can Invest.

Historically, digital currencies have been known to be very volatile—and will likely remain this way as the ecosystem matures. Digital currency is like any investment you are already doing. There's always going to be risks. Advocates see them as the future of finance, critics see them as scams, and a lot of early investors are profiting from the eye-popping returns generated in the rapidly expanding world of digital currencies.

It's your decision.

If you eventually choose to invest, then you must strive to protect yourself from any risks by:

- Doing enough research on the platform you are planning to use.
- Consult with a professional adviser versed in digital currency trends.
- Read as much as you can on your own about digital currency.

Thankfully, you have this book.

For anyone looking to cash in on these opportunities, investments can be made in three primary ways:

In the companies building businesses in the emerging space;

Buying the cryptocurrencies out-rightly;

Researching well, the investment funds being created to hold digital currencies perhaps for a long haul.

For a direct investment in a digital currency, new investors should look for three traits: ***intrinsic value, longevity and durability.***

Look out for any online currency that has lasted for two straight years without breaking down before committing your money.

Making Money with Cryptocurrency Trading

Rule 1; DON'T BE GREEDY!

Cryptocurrency Trading is the Forex (*Foreign Exchange*) of cryptocurrencies.

This means, you are able to trade different bitcoin and altcoin normally for USD and BTC.

Cryptocurrency Trading is an alternative way to get involved in the Crypto-World and making good profits! But you must curb your greed in other to succeed.

Greed has a way of bringing out tears from a victims eyes.

Know when it is OK to take your profit and let the others go.

It is very possible to make a lot of money trading Cryptocurrency pairs, just like forex traders do trading fiat currencies. There are two major types of traders in the Bitcoin/ Crypto market, they are ***'long term'*** traders and ***'short term'*** traders. Each of these group of traders are classified by how long they may wish to hold onto a given position of trade.

Long term traders are usually involved in studying price trends over long periods of time. This informs their decision to buy and hold bitcoin also over long periods with the hope of taking profit at a price higher than their original entry point. With Bitcoin still in its developmental stages, a lot of users suggest that this is a good time to buy.

This suggestion is based on the assumption that with increasing use case scenario and more adoption, demand for bitcoin or any other crypto currency, like ethereum and their associated technology will increase, thereby creating

more demand for the cryptocurrency which will automatically cause an eventual increase in value.

Glimpses of this have been observed with the surge in bitcoin price which coincides with a boost in its market capitalization and volume of trade.

On the other hand, short-term traders analyze the inter-day behavior of bitcoin prices and seek to take advantage of the swings in price.

These traders thrive in market volatility, a factor that is presently characteristic of Bitcoin.

Short time traders are also high risk takers.

High Risk = High Reward

Why trade bitcoin and not Forex?

Easy to enter

To start trading bitcoin and earning money, you really need less than an hour. If you want to start trading Forex, you need to open an account – this takes several weeks until they send you the sign up forms and access code. Then it takes some days until you transfer some money from your bank account to your Forex Broker.

We should not forget, that crypt-trading is also easy to leave. You just transfer your bitcoins out of the exchange into your wallet and you are done. We don't even want to start talking about how nerve-racking it is to quit your broker.

The Different ways you can Profit from Cryptocurrency Price Movements

Spot Trading

Bitcoin spot trading platforms let users buy and sell bitcoin against a fiat currencies. You can deposit USD, CNY, EUR, JPY, AUD, CAD or INR to invest in bitcoins; or deposit bitcoin to sell for your local currency.

Example exchange: **COINBASE.COM, LOCALBITCOINS.COM**

Margin Trading

Bitcoin margin trading is borrowing bitcoins or a fiat currency to trade in a live spot market. While margin trading you post collateral in BTC or USD and pay daily interest on your loan until your trade is closed.

Example Exchange: **WHALECLUB.CO, CEX.IO, BITFINEX.COM**

Futures Trading

Bitcoin futures platforms let you trade the price of bitcoin sometime in the future. Most bitcoin contracts settle either weekly, biweekly or quarterly. Bitcoin future trading is high leveraged and more volatile than spot markets. Most derivatives have a settlement date on which all contracts are finalized and your position is liquidated. Bitcoin derivative markets allow traders to leverage their position and make a profit whether the price of bitcoin goes up or down. When your trade ends the loan is repaid and you keep all the profits.

Example exchange: **CRYPTOFACILITIES.COM, BITMEX.COM**

Options Trading

Bitcoin options lets you bet whether the price of bitcoin will be higher or lower at some time in the future. Unlike bitcoin futures, you cannot settle the position any time. Your trade either wins or loses the maximum once the expiry time is reached.

Example exchange: **COINUT.COM**

Trading basics.

Researching the market is referred to as ***"fundamental analysis."*** By gaining the right information at the right time and understanding how it will interact

with the market, it becomes easier to stay predict trends — essentially whether or not a crypto currency will rise or fall.

In addition to fundamental analysis, you also have ***"technical analysis."*** Technical analysis is equally important, but it refers specially to studying charts and finding patters—for example, at a certain price, a coin will fall repeatedly.

The most basic but important thing to remember about trading, any trading is: ***Buy low, Sell high.***

If prices fall at the local grocery market everyone goes to buy as it is seen as a great deal. But if prices fall in the crypto market everyone sells in fear.

Learn how to act tactically not emotionally.

Buy the rumor, sell the news.

When major news sites publish articles it is usually exactly the right time to actually get out of the trade.

Safety rules were written with blood.

That statement sounds familiar to every soldier around or Boy Scout. Although we are not dealing with a risk to human lives, but losing your expensive bitcoins by making mistakes while trading is definitely not a fun situation.

I know.

So, how can we avoid those mistakes in our trading?

First, it is important to note that to trade right requires attention and your one hundred percent focus.

Secondly, trading is not for everyone.

The following tips are easy to internalize because these tips were ***"written in blood" (my own blood).***

However, it's still difficult to apply them in real-time.

After all, we are not rational human beings.

1. Have a reason before entering each trade: Start a trade only when you know why you're starting and have a clear strategy for afterwards. Not all traders make gains from trading. The cryptocurrency market is driven by large whales *(yes, the same ones responsible for placing huge blocks of hundreds of Bitcoins on the order book)*. The whales are just waiting patiently for innocent little fish like us to make mistakes. Even if you aspire to trade on a daily basis, sometimes it is better not to earn and do nothing, instead of jumping into the rushing water and exposing your coins to losses. From my experience, there are days where you only keep your profits by not trading at all!

1. Target and stop when starting a trade: For each trade you must set a clear target level for taking profit and more importantly, a stop-loss level for cutting losses. A Stop-loss is setting the level of loss where the trade will get closed.

1. Meet FOMO ***(fear of missing out)***: Indeed, it really isn't fun to see such situations from the outside – when a certain coin is being pumped up like crazy with huge two-digit gains in minutes. True, it's possible that many may have caught the rise ahead of us and it can continue rising, but bear in mind that the whales (as mentioned above) are just waiting for small buyers on the way up to sell them the coins they bought in cheaper prices. Prices are now high and it's clear that the current coin holders only consist of those little fish. Needless to say, the next step is usually the bright red candle which sells through the whole order book. Hehehehe funny!

1. Risk Management: little pigs eat a lot, big pig gets eaten. This statement tells the story of the market profits from our perspective. To be a profitable trader, you never look for the peak of the movement. You

look for the small profits that will accumulate into a big one.

1. The underlying asset creates volatile market conditions: Most cryptocurrencies are traded according to the bitcoin value. Bitcoin is a volatile asset (relative to FIAT) and this fact should be taken into consideration, especially in the days when the bitcoin value is moving sharply. Bitcoin and altcoins have an inverse relationship in their value, i.e. when the value of bitcoin rises then altcoins are losing their bitcoin value, and vice versa. When bitcoin is volatile, our conditions for trading are kind of foggy.
2. During fog we can't see much ahead, so it is better to have close targets for our trades or not to trade at all.

If you are only interested in trading altcoins, then, note the following:

Most altcoins lose their value over time. They simply bleed their value away slowly (sometimes rapidly). As a rule, never trade any altcoin that has a total market capitalization of less than $100,000. ***The whale can easily manipulate those.***

Take this into account when holding altcoins for the medium and long term, and of course choose them carefully. What kind of altcoins are recommended for the long term? Remember, this is only when there is a reason for making a trade. The projects/ coins that have a higher daily trading volume and which have a widespread community behind them, with continuous development, are here to stay with us.

Ethereum ETH, Monero XMR, Factom FCT, DASH, are all leading coins and traded the most volume daily.

You should follow the coin's chart and identify low and stable periods. Such periods are likely to be a consolidation period by the whales, and when the right time comes, accompanied by a good press release of the project, the pump will start and they will sell in profit.

A word about public ICOs (crowd-sales):

Many new projects choose to make a crowd-sale where they offer investors an early opportunity to buy a share of the project (tokens or coins) in what is meant to be a good price for the tokens.

The motivation for the investors is that the token will be traded from day one on the exchanges and would yield a nice profit to the ICO participants. In recent years, there have been many successful ICOs, both the project itself and especially in measuring the yield for investors. Coins doubled, or tripled, their value and much more in relation to their value on the crowd sale. Okay, but what's the catch here? Not all the projects benefit their investors. Many ICOs prove to be complete scams, not only were they not being traded at all but some projects disappeared with the money and we have not heard from them right up to this day. I know this by personal experience.

So how do you know if you should invest in an ICO? It's not about science, it is important to pay attention to the level of seriousness of the project and its team. Look for the project's website (does it look like a child has built it during computer school?), who is the team behind the project – Are they hiding behind nicknames or proudly present themselves on their website? Pay attention to the Bitcointalk thread (does it exist at all?) and ***how the team members respond to technical questions.*** Is there a large community behind the project? Expect to see a Slack gathering its community. Watch out the amount raised: A project which had raised too little will probably will not be able to develop over time, a project which had raised huge amount – there won't be enough investors left out there to buy coins on exchanges.

And most importantly is risk management. Never put all eggs in one basket and invest too much of your portfolio in one ICO if you are investing at all.

I will talk more about ICOs in a subsequent section.

Crypto Trading Robots

Trade While You Sleep

Trading Bots have been used in computational trading since the seventies. They are called bots because the programs execute trades like humans do, but they do it autonomously and can operate continuously without having to rest.

Trading bots or algorithmic trading is a technique that uses pre-programmed software that analyzes market actions, such as time, price, orders, and volume. They are used within many global stock exchanges and is a legal practice for the most part. Bitcoin trading bots are said to establish more efficient trading and can be utilized on many well-known cryptocurrency exchanges today. There are free bots that can be downloaded online. Some people have also designed their own bitcoin trading bots. There are also trading bot subscription services, offered by various trading engine and programming companies.

There are many different businesses online offering these bot services, and some of them may not be legitimate. Many of them are pure scams, and some may have malicious codes that can steal your money. People should research diligently before trusting any free bot software. Finding reputable and functioning trading bots may increase trade profits, if used correctly. Do your due diligence before trusting a machine!

If you are looking for a magical bot that you will just click a button and it makes you rich overnight, sorry, there is no such bots, especially if you don't even know much about trading cryptos in the first place.

Trade robots can help you a lot in trading and watching the market and earning profit ONLY if they are coded well and you know how to use them based on your knowledge of the market.

Some examples of trading bots;

Haasbot, BTC Robot, Cryptotrader, My Bitcoin Bot, CryptoArbitrager.

Again, Beware of Bitcoin Whales

Bitcoin whales are individuals or groups who hold vast quantities of bitcoins and can sometimes sway the market towards their preferential price.

There are many trading maneuvers *whales* use to profit. For instance, they could use a trading tactic commonly called the *'rinse and repeat cycle.'* The rinse trade is used in many types of markets and can be effective if timed correctly and very profitable if you are a bitcoin whale.

How it works.

First of all, whales understand that most traders, often make emotional decision in their trades. So they capitalize on such weakness to profit massively.

The trader with a lot of holdings starts selling bitcoins at a price lower than the market rate. This move, most of the time cause a panic sell-off by small-time traders. The trick is that after the whales have sold below the prevailing market value, enough for panic ensue, they then crutch, wait and observe the panic-selling take place until the bitcoin price reaches a new low. At this point, the whales quickly scoop up way more bitcoins than they first started with. This process is repeated over and over by the whales, until they devastate overtly emotional small traders.

Whales may not just be individuals, they large organizations like a bitcoin investment fund as well.

How many bitcoins does it take to be a whale? From 1,000 to 25,000 bitcoins will make you a whale. And you will smile to the bank as often as you wish.

Another method whales use in manipulating cryptocurrency markets is by utilizing ***buy and sell walls.***

In cryptocurrency markets, exchanges use an order book to facilitate trades where a buyer can set up an order to buy or sell at a specified price other than the spot price. For instance, if the market drops traders will usually buy at a lower bid and sell if the price reaches a higher level. In order to place an order in the exchange's order book, you have to legitimately own enough funds to cover the order. This means a whale and even smaller traders in many ways can bluff and make it seem like a buy or sell walls exist. However, often times large buy and sell walls disappear just before the price gets close enough because a big player was just bluffing. Nevertheless many buy and sell walls are very real and can change the odds rather quickly if they manage to liquidate someone's assets.

Sometimes whales don't purchase or sell on traditional exchanges because their holdings or orders could cause a stir in the market. For cryptocurrencies over the counter trading ***(OTC)*** or "***dark pools"*** is where big buyers and institutional traders can purchase vast amounts of bitcoins without being seen by the public eye. Dark pools are similar to OTC trading as they are usually found on exchanges that enable '***off the record'*** trades which ensures a whale's moves are more private. Typically OTC markets and dark pools only allow traders who purchase an abundant amount of bitcoin at one time and set minimums for entry.

The lesson here is never panic sell.

Buy when everyone else is selling, sit on your coins until you really need the money.

Making Money from Cryptocurrency Lending on Exchanges

On some exchanges, you are allowed to lend bitcoin (or any other cryptocurrency) to the people trying to go short (bet that the currency will fall). It's very similar to p2p lending, but instead lending bitcoin to people who are going to invest it in some unknown activity, you are lending to people who trade.

This kind of lending is not called p2p (person to person) due to the fact that you can't choose the person who you borrow to. You don't know who received your bitcoins and everything is managed by the cryptocurrency exchange.

What are the benefits of crypto lending?

There are many benefits of borrowing your money on crypto-exchanges to margin traders. The key benefits of this kind of investment are:

Low Risk – The borrower can't scam you and he can't take out the bitcoins out of the exchange.

Good Return of Investment – It's about 0.02% per day (more or less depending on the currency). This sums up to a total of 0.0002*365 = 7.3% per year!

Less time required – you don't need to search for the best lending possibility, because it's all about lending to traders. You don't need to investigate the person etc.

Bonus earning upon trading – For example, if you are long on Ethereum and think you will stay on this position for at least one week, then why not just lend your current Ethereum? You will receive extra returns on your invested capital.

Self-Managed – all the payments are automated, you won't need to chat with nobody.

Best Platforms to lend Bitcoin or any other cryptocurrency

Here is a list of the top margin funding platforms you can use. Currently, I do my lending mainly on the
Poloniex Exchange and bitfinex.com.

If you are too lazy to handle this manually, you can always try the Poloniex Lending Bot. For only 10% of your lending profit, it will make everything automatically.

Can you lose your money by lending on exchanges?

People cannot take your bitcoin and run away. So it's not possible for borrowers to lose everything they have. If their trading position is at a loss, they will cover the loss with the funds in his trading account. The funds in the trading wallet serve as a collateral only, meaning that a trader's position is force liquidated, if the value of his account falls below the maintenance margin. This maintenance margin guarantees that lenders will get their coins back.

The only risk on margin funding: **the exchanges!**

The hazard on lending bitcoins on exchanges is only in terms of the exchanges themselves scamming you.

This means, that the owners of the exchanges can decide to disappear and run away with all the coins people invested into their trading wallets. Another risk is the exchanges getting hacked.

It does not happen all the time, but the possibility is there so beware!

Tips on Margin Funding

Open accounts on more than one exchange – this will reduce the only risk you have: to get scammed by the exchange. Furthermore you will be able to

lend more cryptocurrencies.

Choose your Rate (%) smartly – Always check out what the lowest offered lending percentage is, and select 0.001% less than it. This way your crypto currency won't wait for a long time to get a borrower, hence will maximize your earnings.

Choose your lending period wisely – If you don't have time to check every day for the best possible interest rate, than you should lend your funds for 15-30 days.

See if you trust the cryptocurrency – To lend coins, you need to have those coins. This means, if you want to lend STR (star) Coins – because they have the best daily return rate – then you need to buy them before lending them. This means, you will be holding on the STR coins for some period of time. Therefore you should only lend coins that you trust and think will gain on value with time.

Making Money from Cryptocurrency through Mining

Is it possible to earn money through Cryptocurrency mining?

As a hobby venture, yes you can generate a small income of perhaps a dollar or two per day. In particular, Ethereum, Litecoins, Dogecoins, and Feathercoins are very accessible for regular people to mine, and a person can recoup $1000 in hardware costs in about 18-24 months depending on the market value of the coin mined.

The ***21.co*** project has enables developers and hobbyists to use Raspberry Pi 2 or 3 to mine small amount of Satoshi to run experimental projects.

You ca look at the website ***http://21.co*** for that information.

Start a Bitcoin full node on your Linux, Mac, BSD or Windows system to mine bitcoin *(help validate and relay transactions across the Bitcoin network)* by running this command:

curl https://bitnodes.21.co/install-full-node.sh | **sh**

Can I make money mining Bitcoin now?

If you had started mining Bitcoins back in 2009, you could have earned thousands of dollars by now. At the same time, there are plenty of ways you could have lost money, too, because it was never a smooth upward journey all through.

For now, bitcoin mining is reserved for large-scale operations only. Over the past five years, the mathematical difficulty of discovering bitcoins has

grown far beyond what a regular individual can achieve at home with the best of desktop, laptops or GPUs. The current up-front investment and maintenance cost to mine bitcoins is no longer worth it for small-scale consumers.

Unless you are willing to spend tens of thousands of dollars on industrial hardware and rent an air-conditioned office to house your hardware, there is no profit in mining bitcoins.

So we will focus on the profitable cryptocurrencies that is minable by an average person.

Ethereum, Litecoin, Feathercoin, Monero, Dash and Dogecoin are still very profitable to mine because all of them are gaining traction and GPU mining them is possible. *Litecoins, Dogecoins, or Feathercoins are 'scrypt' coins.*

You can use this website https://www.cryptocompare.com/mining/calculator/btc, to check how much you can make with your hardware investment.

Bitcoin Mining Hardware

CPU

In the beginning, mining with a CPU was the only way to mine bitcoins and was done using the original Satoshi client. In the quest to further secure the network and earn more bitcoins, miners innovated on many fronts and for years now, CPU mining has been relatively futile. You might mine for decades using your laptop without earning a single coin.

GPU

About a year and a half after the network started, it was discovered that high end graphics cards were much more efficient at bitcoin mining and the landscape changed. CPU bitcoin mining gave way to the ***GPU (Graphical Processing Unit)***. The massively parallel nature of some GPUs allowed for a

50x to 100x increase in bitcoin mining power while using far less power per unit of work.

While any modern GPU can be used to mine, the AMD line of GPU architecture turned out to be far superior to the nVidia architecture for mining bitcoins and the ATI Radeon HD 5870 turned out to be the most cost effective choice at the time. Nowadays, GPU manufacturing companies are making cryptocurrency specific GPUs which deliver much better performance compared to regular ones.

FPGA

As with the CPU to GPU transition, the bitcoin mining world progressed up the technology food chain to the ***Field Programmable Gate Array (FPGA)***. With the successful launch of the Butterfly Labs FPGA 'Single', the bitcoin mining hardware landscape gave way to specially manufactured hardware dedicated to mining bitcoins.

While the FPGAs didn't enjoy a 50x - 100x increase in mining speed as was seen with the transition from CPUs to GPUs, they provided a benefit through power efficiency and ease of use. A typical 600 MH/s graphics card consumed upwards of 400w of power, whereas a typical FPGA mining device would provide a hashrate of 826 MH/s at 80w of power.

That 5x improvement allowed the first large bitcoin mining farms to be constructed at an operational profit. The bitcoin mining industry was born.

ASIC

The bitcoin mining world is now solidly in the ***Application Specific Integrated Circuit (ASIC)*** era. An ASIC is a chip designed specifically to do one thing and one thing only. Unlike FPGAs, an ASIC cannot be re-purposed to perform other tasks.

An ASIC designed to mine bitcoins can only mine bitcoins and will only ever mine bitcoins. The inflexibility of an ASIC is offset by the fact that it offers a 100x increase in hashing power while reducing power consumption compared to all the previous technologies.

Unlike all the previous generations of hardware preceding ASIC, ASIC may be the "end of the line" when it comes to disruptive mining technology. CPUs were replaced by GPUs which were in turn replaced by FPGAs which were replaced by ASICs. There is nothing

known yet, to replace ASICs now or even in the immediate future. But alas, I heard that quantum computers are on their way. We patiently await their arrival.

Mining profitability is also dictated by the exchange rate, but under all circumstances the more power efficient the mining device, the more profitable it is. If you want to try your luck at bitcoin mining then try this website https://asicminermarket.com/ is probably the best deal. To calculate your mining equipment profitability use this website: https://www.nicehash.com/index.jsp?p=calc and https://www.cryptocompare.com/mining/calculator

Mining Software

There are two basic ways to mine: On your own or as part of a bitcoin mining pool or with bitcoin cloud mining contracts and be sure to avoid bitcoin cloud mining scams. There are too many out there. Almost all miners choose to mine in a pool because it smoothens out the luck inherent in the bitcoin mining process. Before you join a pool, make sure you have a bitcoin wallet so you have a place to store your bitcoins. Next you will need to join a mining pool and set your miner(s) to connect to that pool. With pool mining, the profit from each block any pool member generates is divided up among the members of the pool according to the amount of hashes they contributed.

1. **AntPool:** Antpool is a Chinese based mining pool, maintained by BitMain. Antpool mines about 15% of all blocks.

2. **DiscusFish/F2Pool:** DiscusFish, also known as F2Pool, is based in China. DiscusFish has mined about 12% of all blocks over the past six months.

3. **BitFury Pool:** BitFury is one of the largest producers of Bitcoin mining hardware and chips.

BitFury currently mines about 12% of all bitcoins in three data centers across Georgia.

It's a private pool and can't be joined.

4. **BTCC:** BTCC is China's third largest Bitcoin exchange. Its mining pool currently mines about 7% of all blocks.

5. **ViaBTC:** ViaBTC is a somewhat new mining pool that has been around for about one year. It's targeted towards Chinese miners.

6. **BW Pool:** BW, established in 2014, is another mining company based in China. It currently mines about 8% of all blocks.

7. **BTC.Top:** BTC.top is another new pool. It does not appear to have a website, so it may be a private pool.

8. **Slush:** Slush was the first mining pool and currently mines about 6% of all blocks.

Cloud Mining Services

Bitcoin cloud mining, sometimes called cloud hashing, enables users to buy the output of Bitcoin mining power from bitcoin mining hardware placed in remote data centers

Then all Bitcoin mining is done remotely in the cloud. This enables the owners to not deal with any of the hassles usually encountered when mining bitcoins such as electricity, hosting issues, heat, installation or upkeep trouble.

What are Bitcoin Cloud Mining Advantages?

No excess heat to deal with.

Quiet because of no constantly humming fans.

No electricity costs.

No bitcoin mining equipment to sell when bitcoin mining is no longer profitable.

No ventilation problems with hot equipment.

No pre-ordered bitcoin mining hardware that may not be delivered on time by bitcoin mining equipment suppliers.

What are Bitcoin Cloud Mining Disadvantages?

FRAUD!!!

Unverifiable or otherwise shady bitcoin cloud mining operations

No fun! If you like building your own bitcoin hashing systems.

Lower profits – bitcoin cloud mining services or mining company will have expenses bitcoin mining contracts and may cease operations or payouts in the contracts if the bitcoin price is too low

Lack of possession of the bitcoin mining hardware

Lack of ability to change the bitcoin mining software

Hash Rental Services

Hash rental services lets bitcoin and altcoin miners list their hardware on website marketplaces for hourly leased contracts, which prospective renters can view and purchase a contract from owners of the hardware.

Renters can view the list of hardware available for lease, and purchase an hourly contract from the rig owner, enabling people without the hardware to gain access to a wide range of available bitcoin or altcoin miners. This mining ,to me, is profitable when mining new and less expensive currencies. After all, if the mining was profitable to hardware owners, they will most unlikely give out the hash power to someone else. So research very well before you throw you money away. That said, you can check out the following sites; https://www.nicehash.com, and https://www.miningrigrentals.com

How to set up your own Ethereum mining rig

Mining ethereum is still very profitable, at least for now. Note also that there is a plan for ethereum to move away from ***PoW*** to ***PoS*** mining algorithm, sometime in future. This is because ethereum prices has been soaring in the last three months. For instance, in January 2017, ethereum price was less that $12, but by the end of June, 2017 ethereum price has risen to about $400 before dropping again to the $300 range. That's over 6,000% increase. Crazy ehh? Yes. It happens.

Make sure you have stable power source.

I do configure off-grid configure Solar kits for mining. Reach out if you need one.

So what will you need before you can start minting money with your mining rig?

This also goes for mining other altcoins with good value.

1. Motherboard. Your motherboard should not be all these run-off-the-mill kinds of boards. You need good quality motherboard, the type they use for PC gaming. It should also have a good processor. The main feature you are looking for in a motherboard is the number of GPU slots it has as this will determine how many graphics cards or GPU's it can fit - and in the end your total hashing power. So get the one that has at least 4 PCI slots.

Hard disk: Of course you will need a good HDD. That is where the blockchain records and other mining tools you will download will live. So get a fat one. 500 GIG will work fine.

2. GPU Cards: GPU stands for Graphic Processing Unit. This what will determine the total hash power you will need, so you will need to spend a lot of time searching for them in the local computer market or online. You are

most likely to get them from dealers on gaming products. Traditionally GPU cards are used for high resolution graphic games. The GPUs come in different memory capacity. Your best bet is to acquire the ones that have up to 8GIG.

You can choose from this list below:

The ***Radeon R9 295X2*** has by far the highest hash rate (46.0 MH/s) of the Ethereum GPUs on the market and will cost you $600. It has a power cost per day of about $1.44, a return per day of about $1.61 and a cost per MH/s of $13.04. This gives a return per year of $586.43.

A ***Radeon R9 HD 7990*** will cost you $680. Its power cost per day is lower than the R9 295X2 at $1.08 but its hash rate is significantly lower at 36 MH/s. Its return per day is $1.29 while its cost per MH/s is $18.89, giving it a return per year of $469.40.

The ***Radeon RX 480*** is most arguably the most economical in terms of cost and saving electricity. Its power cost per day is significantly lower than the two that I have mentioned at $0.4320. Its hash rate is 25.0 MH/s, meaning its cost per MH/s is $7.96. This gives a return per day of $1.21 and therefore a return per year of $440.91. Radeon RX 480 will cost you $199.

A ***Radeon RX 470*** has a modest hash rate of 24.0MH/s. Its power cost per day is exactly the same as the Radeon RX 480 at $0.4320. Its cost per MH/s is $9.13, giving it a return per day of $1.15 and a return per year of $418.16. Radeon RX 470 will cost you $219.

3. Power supply/ Casing: You must choose the power supply carefully. You need to sum up the power consumption of your GPU and all the other components and make sure your power supply has the capability to supply more! So if you have two GPU's that consumes 220 Watts and other components that need 250 Watts then you can get away with a 750 Watt power supply unit as the total power needed is only 690Watts. So spend time and work this aspect out with a good electronic/ electrical tech guy to avoid heart attack.

4. Operating system/ mining Software: Choose your operating system, windows or Linux. I have outlined the differences between open-source and

closed source elsewhere. Make your choice. Remember to install the drivers properly. EthOs is the *de facto* mining software for mining ethereum.

After setting everything up, next is to get a good ethereum wallet. Myetherwallet.com is great and easy to setup. Choose between Solo mining and Pool mining. Pool mining will pay you best. So point your hash power to the pool service you have chosen. They will give you all the parameters you need to connect successfully.

That is it. You are now set to start minting ether!

Creating your own Cryptocurrency

Local Digital Currencies may be the burgeoning field of cryptocurrency. These are hyper-local currencies for specific neighborhoods, cities, events, venues, and groups of people that are built around a community of like-minded consumers allowing them to trade freely, quickly, and securely for goods and services that are important in their lives instead of having to rely on the central banks and larger markets to tell them what arbitrary item, be it a copper coin or a piece of paper, holds value.

Feathercoin as a local currency that may have the potential to serve a global market. So a crypto currency global dominance should not be your target if you wish to create your own crypto.

The first step towards creating your own digital currency is to **find a community** that it will add value to in an organic manner, and build the currency around them rather than building a currency and expecting everyone to show up and start using it. It has to be sensitive to their needs and be relevant to their cultural heritage and background. It's like building what your customers need not what you think they want. So a devoted community of users is key.

Since virtually every cryptocurrency on the market today is based on the open source code of either Bitcoin or Litecoin that is available on GitHub, the second step, which is **creating the code;** is actually easy. You just need a developer or developers skilled in C++ programing language to help you build in your own unique features. You need to determine the mining technique; proof of work (PoW), or proof of service (PoS) etc. You must decide on the hask algorithm to use SHA256 or Script. In coding, the most complex steps may be related to how complex you plan to have the individual parameters of the blockchain. For example, many currencies just use the litecoin code and copy it, but with *Quark* there was a whole new Hash

algorithm–that is to say, it's separate from both bitcoin and litecoin–so this aspect, if you were to change it, would certainly be the most difficult part and time consuming. In this case coding your own cryptocurrency could take months and a lot of money. But if a developer is just forking and reusing code from GitHub and changing some simple parameters, that's something a competent coder could do in literally 30 minutes.

We call it ***forkology!*** *A simple act of forking a repository and quickly re branding it as your own product… beautiful money maker — No prior knowledge is required!*

Remember, you have a duty of care at the development end in terms of bug fixing and ensuring the promise made at launch but you also have a duty to educate people of the risks and give them what they need to secure their wealth.

The next step is to bring Miners On-board

Once you have developed your coin, you need to spread the word so people start mining it, which raises awareness of its existence and hopefully begins to gain some value in the eyes of its miners and users. This is where makers of cryptocurrencies need to stop thinking like coders and instead look into how human beings put trust (and value) in things. The mining reward must be attractive else miners will not be attracted to it.

You need a group of loyal miners committed to the cause who will process your payments even during slumps in price because they believe in the eventual outcome. It's about good communication and team building.

So you have conceptualized a good cryptocurrency and brought in the right team together to code and nurture it along its way. You've spread the news around the cryptocurrency forums and there's a healthy dose of miners actively working to grow your currency. The next step is **marketing your currency** so all the people mining it or holding it, have a place to spend it. This is no small feat. After all, you need to convince individuals and merchants that these digital bits you've created hold value and can be traded for things, just like traditional, trusted money. It's a process of confidence building. You can take it to the *Cryptocurrency market place* to find the exact

target group your coin will appeal to. It's about inspiring people to learn and discover the advantages of using your coin for themselves. Money is a ledger, it is a tool that people will use as a way of achieving their goals and satisfying their needs. They must see this for themselves in your coin. Merchants mainly have three principal aims: to make money, to save money, and to increase their awareness. If you can bring them customers and increase their sales while reducing their payment fees, the rest is a matter of persistence.

So that is it at its most basic level about creating your own crypto.

So how does it profit me? Someone may ask.

Well, you defined the total block mining rewards, Block halving rate (for PoW), the total number of minable coins, the total number of pre-mined coins, yearly Interest % (for coins with POS) and minimum/ maximum Stake Age (For coins with POS). In setting all these parameters, you will have taken care of your personal financial future before inviting others.

As one popular parlance goes; He that is holding the yam and knife determines everyone's share.

What is an ICO?

An ICO is a recently emerged concept of crowdfunding projects in the cryptocurrency and blockchain industries, an alternative to the Venture Capital concept.

ICO stands for Initial Coin Offering. It is an event, sometimes referred to as 'crowd sale', when a company unveils its blockchain project or its own cryptocurrency with a purpose of raising needed funds for the execution of the project. It usually releases a certain number of crypto-tokens and then sells those tokens to its intended audience directly at a discounted rate in exchange for Bitcoins or ethereum, but it can be fiat money as well.

Through this process, the company gets the capital it needs to fund its product development and the audience members get their crypto tokens' shares. Plus, they have complete ownership of these shares.

ICOs can be compared to IPOs (Initial Public Offering) in the sense that both have the same goal; to source and raise fund for projects from the public. One of the things that makes ICOs unique is that it is border-less, transparent and is driven by digital currencies. But regarding IPOs, a company's shares, released during an IPO, always denote a share of ownership in the respective company. This is not, by default, a case with crypto-tokens that are sold to the public in an ICO. Crypto-tokens can be used to transfer voting powers - a larger share of tokens giving more voting power.

The other crucial difference is that IPO's are heavily regulated by the government. This requires a partaking company to prepare large amounts of paperwork before releasing its shares. It also implies severe consequences in the case of non-compliance. Conversely, cryptocurrency crowdfunding is a new scene, largely untouched by government regulation. That means that any

project can launch an ICO at any time with little preparation and any person can take part in it and contribute their money, no matter what country they are from. This liberal environment carries both new opportunities and risks when compared to the more conservative IPO's.

Profiting from ICOs

Typically, the crypto-tokens released during an ICO are sold at a fixed price denominated in bitcoins or US dollars. That price is not usually backed by anything but the community's faith in the development team to release a finished product at some point in the future, so tokens are highly discounted. Sometimes as much as 50% less than actual value at the ICO's lunch time. After the project is developed and launched, the tokens' value becomes secured by a real, working product. And that almost always leads to an increase in price. At this point, a lot of people who didn't get the opportunity to buy the token at the ICO will want in on the project's success. When this happens, the original backers may sell their tokens for a nice and substantial profit.

For example, during the ICO of Ethereum in 2014, the tokens were sold at a price ranging from $0.3 to $0.4 per token. After the project's main platform was released in July 2015, the price of each token had risen significantly, reaching as high as $19.42 at one point. This means that some of the luckiest participants were able to claim an ROI of over 6000 percent.

It is important though that you should keep in mind that profits are not guaranteed. It's a risk that participants must be aware of before joining. An ICO campaign may fail and in that case, all contributions will be returned to their senders depending on the terms of the project.

Owing to discrepancies in some past ICOs, who took advantage of the unregulated environment to mismanage resources thereby bringing distrust into the system, some companies now impose restrictions on themselves to provide sufficient trust and transparency for the contributors.

Blockchain startup owners realized that without government regulations, it has become their duty to establish the terms that will ensure sufficient trust from the community and, by extension, the sufficient inflow of contributions.

This has resulted in a number of self-imposed restrictions such as;

- *Storing the contributions of the community members in escrow wallets. In order to access the funds stored in an escrow wallet, the owners need several private keys. One of the keys is usually owned by a trusted third party uninvolved in the project development.*
- *Establishing a legal entity for the company and documenting all the terms and conditions of the ICO.*

How to spot an ICO offerings with potential for success.

How do you discern from ICOs with potential opportunities from grab-the-money-and-run schemes?

I normally start by asking the following questions;

What type of token is being issued?

If it is a Blockchain Token (like a new crypto), I will ask further.

Private or Public Blockchain? Scalability? Consensus mechanism? Privacy? Governance? What problems does it solve that previous blockchains before have not solved or could not solve? Purpose of the token? Rights attached? All criteria listed below.

Does it have in-dApp Token

Purpose of the token? Sustainable revenue models of different stakeholders? Rights attached? All criteria listed below.

Is it a DAO token

Does it manage a lot of funds? Splitting mechanism? Governance of Edge Cases? Security? Rights attached? All criteria listed below.

Purpose of the token?

Is it a token with an inherent value or a share?

What will the token be used for? *ETH for gas*, *BTC for payments…*

Is it just an incentive mechanism for the stakeholders?

Does it contribute to a sustainable economy in the blockchain or within the DApp/DAO?

If it is pre-mined, how is the token distribution?

How will be the token distributed after the ICO? How much goes to the founders?

Stage of project?

Landing Page only

White paper

Proof of Concept

If landing page only…

Forget it!

If white-paper

Is it well structured?

Does it explain the technology in depth?

Do they have a road-map?

Does it survive swarm review- expert opinion?

Is it written for marketing reasons?

Does it need a blockchain, or is there an off-chain solution to solving the same problem?

If proof of concept

Does the project have a working prototype or an alpha version before the fund raising?

Were there a lot of commits on github?

Is a Testnet available?

If it doesn't have an alpha version, a well written White-paper and a good team could compensate for the lack of progress.

Security; Auditing

Any external audits of the code?

If it has been running on testnet for some time with no major issues, it is a good sign.

Legal

Does national or international regulation apply?

If yes, how could that effect the business model in the short & long run?

Founders & Team

Track record

Previous projects

Technical know how

Formal education

Community

Do they run a blog/reddit/slack?

How interactive are those social media activities?

Are they reporting progress?

Size of a community depending on stage of project

Market Potential

Core value proposition: What problem does it solve?

How much demand is there for the project, short & long term?

Competitors?

Partners?

Does the project get discussed in the relevant communities even before launch? This could be an indicator for big interest.

Funding Structure

Why does the project need funding at the moment of the ICO?

How were they funded up to that point?

Do they have a cap on the crowd sale?

Is the amount of tokens issued limited to the initial crowd sale?

Are they putting too much money into marketing?

Developing Blockchain Applications

Bitcoin Application Development requires that the developer should possess some of the following coding skills: C++, Java, Objective-C, Python, Javascript, Java, GO and Ruby, depending on the field of development you will want to focus. A comprehensive bitcoin developer reading list can be found here: https://github.com/jashmenn/bitcoin-reading-list

Andreas Antonopoulos book, "Mastering Bitcoin" is tailored completely to developers interested in getting started with bitcoin and block chain development.

You should buy it.

Ethereum Application Development

After bitcoin, Ethereum is currently the crypt-currency with the second largest market cap. In contrast to bitcoin, its blockchain is focused on smart contracts. Ethereum tries to make smart contracts really powerful entities on the blockchain. For that purpose it provides a turing-complete development language call Solidity. *A programing language is called "Turing complete", given that it can run any program (irrespective of the language) that a turing machine can run given enough time and memory.* Its syntax is loosely based on Javascript and thus easier to learn than the bitcoin script. The high level Solidity programs (called "contracts" in the ethereum space) compile down into the actual bytecode that run on the blockchain.

Apart from the lower entry barriers to contract development, Ethereum has a large developer community that works on various aspects of Ethereum. There are different, independent clients (eg.Geth or Parity, to name just the two largest ones) for the blockchain. There are also development frameworks (Truffle or Embark), different development languages (Solidity or Serpent) and nice and useful development/ end user tools (Testrpc, Mist or the Solditiy Realtime Compiler). All of these tools are actively being developed. As such, the environment is a friendly one.

Testrpc is a blockchain simulator. It is easy to install via:
npm install -g ethereumjs-testrpc

Compiling your contract

After contracts are written in solidity, they are then compiled into a script ***(bytecode)*** for the blockchain. After compiling they need to be deployed on the blockchain. A user can use a contract if he knows the contracts address on the blockchain as well as the ABI as a JSON file. *(ABI stands for application binary interface In general, an ABI is the interface between two program modules, one of which is often at the level of machine code. The interface is the de facto method for encoding/decoding data into/out of the machine code.)*

A deployed contract can be used either directly with the right RPC calls or via a wallet like mist. It does not have a useful GUI on its own. To make it user-friendly, we need to provide a frontend to enable users to interact with it in a non-developer way. Such a frontend can be written in HTML/Javascript.

The Web3 Javascript Đapp API library provides access to the blockchain from Javascript.

Frameworks, like Truffle, automate the deployment tasks and allow it to focus on the actual contract and frontend development. So far I have always used Truffle; thus I focus on truffle for now.

Truffle needs to be installed.

If using npm, the installation is a simple.

npm install -g truffle

Deploying a Contract

To deploy a contract to a blockchain, the blockchain must be accessible for truffle. As per the configuration, truffle expects the node to listen on localhost:8545. Thus, before we can deploy a contract with truffle we must start the node. By running testrpc on the console, the node will simulate the in-memory blockchain. By default it listens on localhost:8545, just as truffle expects.

truffle init

truffle migrate

truffle migrate –verbose-rpc

Interacting with the frontend

Truffle already provides us with a web frontend for the Metacoin contract. This frontend can be used to interact with the contract. This is more user-friendly than to expect a user to do the rpc call manually. Truffle can serve the web frontend.

The command is;

truffle serve

It will serve the website and watch for changes in the HTML/JS files. If they are changed, it will redeploy the frontend on the fly. Pointing your browser to http://localhost:8080 will show you the frontend.

That's the steps that it takes to get your contract on the blockchain.

But there is an easy way and, I will show you that one too.

Browser-based IDEs.

The Solidity real-time compiler (https://remix.ethereum.org) and Cosmo (http://cosmo.to/) are both a fast way to get started compiling your smart

contracts right away in a browser. I'm not so sure if Cosmo is still working but I use Remix every other day.

Visit this site to read documentation on how to use Remix IDE. https://remix.readthedocs.io/en/latest/

You can find a comprehensive Ethereum reading list from this link: https://github.com/Scanate/EthList

Here is also a Blockchain/ Crypto reading list: http://startupmanagement.org/2017/06/06/the-ultimate-reading-list-for-blockchain-token-and-cryptocurrency-sources/

Bitcoin and Digital Currency Regulation and Taxation.

The creation and maintenance of an enabling regulatory environment for blockchain project development is very crucial and policy makers should not develop a juridical framework that will undermine the dynamism and innovation of the cryptocurrency industry. Bitcoin and other crypto currencies are unfamiliar with the concept of geography. It had border-less on its DNA. They were created primarily to bypass any regulation and any authority's power, in other to empower the end user against any kind of regulator. Bitcoin is relentless: it knows no time zones, nights, weekends, or holidays. It ignores arbitrary rules enforced at geographic boundaries.

The Bitcoin Network, for instance has be functional for 99.95148808% of the time since its inception on January 3, 2009 02:54:25 GMT.

This apparent enthusiasm for blockchain and cryptocurrency should not be stifled by unfavorable classical laws, rather a highly progressive regulatory framework favorable to its flourishing should be put in place by governments. For me, totally regulating these systems is almost impossible considering their decentralized architecture which operates independent of any authority. However, we can regulate the off-chain services like cryptocurrencies exchange markets, the commercial operators such as online wallet providers, in whichever country they operate.

Strong KYC (Know Your Customer), AML (Anti Money Laundering) and foreign exchange laws should only apply when these cryptocurrencies are converted to fiat currencies and vice versa.

Developed countries like Japan, Germany, USA, Switzerland and Ireland have found crypto currencies useful and have regulated it. Japan recognizes virtual currencies as a method of payment and taxes profits from virtual

currency trading. In Germany, virtual currencies are classified as “units of accounts” and commercial Bitcoin platform operators are required to have a license from the German Federal Financial Supervisory Agency.

As long as proper records are being maintained of how virtual currencies are being transferred or converted into fiat currency, maintaining the current status quo about their regulation and seeing how they evolve is not a bad idea at all.

Fiat or Cryptocurrency in general derives its value by trust placed on the underlying system that supports its utility function and maintenance. Must people do not trust the government issued fiat, and that’s why bitcoin and cryptocurrencies in general, hold such a great hope for them.

Policymakers need to tackle the challenges in understanding both the functionality and risks of decentralized cryptocurrency, in order to create an appropriate legal and regulatory framework.

People are always suspicious about new technologies that could change their lives, and it is very easy to demonize something so difficult to understand (due to its technical level).

Regulation that is tailored to traditional financial services or investment vehicles may fail to account for the unique elements of cryptocurrency.

Four areas that regulators should be concerned and focused on for now are;

(1) Information – ensuring that sufficient information for consumers to assess risk is publicly available; (2) Transactions and options for legal redress if anything goes wrong;

(3) Asset protection – solutions or requirements to protect cryptocurrency-based assets from loss or theft; and, assuming that a digital currency protocol reaches a critical size,

(4) Competition – measures to avoid the concentration of operations in few hands.

By so doing, the perfect jurisdiction for the creation of the most favorable environment for blockchain and cryptocurrency ecosystem, would have been created.

Blockchain and Financial Services Sector.

People use trusted third parties in many roles in finance, as custodians, as payment providers, as poolers of risk, i.e. insurers. Trusted third parties in finance provide four functions:

Validating the existence of something to be traded;

Preventing duplicate transactions, i.e. someone selling the same thing twice or ‘double-spending’;

Recording transactions in the event of dispute;

Acting as agents on behalf of associates or members.

If faith in the technology’s integrity continues to grow, then blockchain technology might largely displace two roles of a trusted third party, i.e. preventing duplicate transactions and providing a verifiable public record of all transactions. Emerging applications, such as smart contracts and decentralized autonomous organizations, might in future also permit blockchains to act as automated agents.

Bitcoin, Virtual Currencies and Conspiracy Theories.

Since the beginning of time, humans have always loved to tell 'tall tales' of all sort and Bitcoin and virtual Currencies are not without their own fair share of such tales. Bitcoin is often considered a weird subject because an anonymous developer known as Satoshi Nakamoto created the original software and this has led to many conspiracy-like discussions involving the digital currency.

Some people believe, *(I have met some of them, especially among church folks)*, that bitcoin might have been created by the CIA or NSA, so it can be used for a "***one world currency"*** or to enforce "***the mark of the beast"*** revealed the Bible book of Revelation. The NSA theory actually fit, seeing that they have the capability, the motive, and the operational capacity – they have teams of cryptographers, the biggest and fastest supercomputers in the world, and they tend to see the need. Control!

The Mark of the Beast.

This *Mark of the Beast* story comes the New Testament, book of Revelations chapter 13. In that section, particularly 13:17, it says that people on earth will have to get a mark on their bodies in order to purchase living necessities. The mark is forced upon everyone from "*the great, the small, the poor and the rich."* Now, because society is gravitating toward a cashless society some curious characters believe bitcoin will be the notorious *mark*. This is one reason while bitcoin acceptance, repeatedly hit the walls in some circles. People who hold such believe will like to have anything to do with Bitcoin or any other virtual currency.

That Bible verse states;

"And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name…" Revelations 13:17

How did this theory gain its current traction among these conspiracy theorists?

Quite recently the subject of "*biohacking"* and *microchip implants* have become a popular trend, especially among millennials. Some people in this movement have installed chips into their hands with a bitcoin wallet inside. Now, because Revelations states that people will "*receive a mark in their right hand, or in their foreheads,"* some consider this the missing link of bitcoin and the mark of the beast connection.

But one of the key elements of the *Mark of the Beast* is to be able to prevent those that refuse to take the mark, from buying and selling. But Bitcoins and Virtual Currencies are decentralized and naturally will prevent any such control. The Bitcoin protocol was designed to resist any kind of control and prevent authoritarianism. Remember the 51% attack we talked about in a previous chapter. The "*mark of the beast"* conspiracy theory gets knocked off at this understanding.

In reality, this theory of bitcoin being the "*mark of the beast"* might even be the opposite of what might really happen. Bitcoin might be a way people can fight the beast, because the beast is authoritarian in character, going by the Bible description of his personality and will try without success to manipulate the bitcoin protocol for it selfish purposes.

One World Currency

Another story conspiracy theorists have up their sleeves is the "*One World Currency"* scheme. They speculate the theory that the whole world will share one single currency, and that purported "currency" is bitcoin. Again this conjecture is again tied to the "cashless society" progression.

They believe that because Bitcoin transactions are not anonymous, and all transactions on the blockchain is traceable and immutable, and also the technology being an integral part of the '*cashless society'* paradigm shift — Bitcoin will likely be that "*one world currency."*

The introduction of the Euro, a currency that covers many countries in Europe, was considered the beginning of this effort. However, in recent times certain countries like Britain, for example, have distanced itself from the Euro during the Brexit vote. As far as bitcoin is concerned, it is becoming the world's *goto* reserve currency, some even forecast that it might be the sixth largest reserve currency by 2030.

To some of these theorists, bitcoin is just another catalyst towards the cashless one world currency secretly crafted by the elite.

Whether this or any other of the many bitcoin conspiracy theories will become a reality, is still to be seen.

Blockchain and Cryptocurrency Lingo

To do my part in helping solve the awareness and enlightenment problem, I have complied a dictionary of the terminology most commonly used in the blockchain space ***(with the help of Wikipedia, GitHub, and TechTarget).***

I hope this serves as a valuable resource for those interested in learning and contributing to the blockchain revolution.

1. **Addresses (Cryptocurrency addresses)** are used to receive and send transactions on the network. An address is a string of alphanumeric characters, but can also be represented as a scannable QR code.
2. **Agreement ledgers** are distributed ledgers used by two or more parties to negotiate and reach agreement.
3. **Altcoin** is an abbreviation of "bitcoin alternative". Currently, the majority of altcoins are forks of bitcoin with usually minor changes to the proof of work (POW) algorithm of the bitcoin blockchain. The most prominent altcoin is Litecoin. Litecoin introduces changes to the original bitcoin protocol such as decreased block generation time, increased maximum number of coins and different hashing algorithm.
4. **Attestation Ledgers** are distributed ledgers that provide a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.
5. **ASIC i**s an acronym for "Application Specific Integrated Circuit". ASICs are silicon chips specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems to mine new bitcoins.
6. **Bitcoin i**s a well known cryptocurrency, based on the proof-of-work blockchain.

7. **Block ciphers a**re a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data at once as a group rather than to one bit at a time.
8. **Block height** refers to the number of blocks connected together in the block chain. For example, Height 0, would be the very first block, which is also called the Genesis Block.
9. **Block rewards** are rewards given to a miner which has successfully hashed a transaction block. Block rewards can be a mixture of coins and transaction fees, depending on the policy used by the cryptocurrency in question, and whether all of the coins have already been successfully mined. The current block reward for the Bitcoin network is 12.5 bitcoins for each block.
10. **A central ledger** refers to a ledger maintained by a central agency.
11. **Chain linking** is the process of connecting two blockchains with each other, thus allowing transactions between the chains to take place. This will allow blockchains like bitcoin to communicate with other sidechains, allowing the exchange of assets between them.
12. **A cipher** is the algorithm used for the encryption and/or decryption of information. In common language, 'cipher' is also used to refer to an encryption message, also known as 'code'.
13. **Confirmation** means that the blockchain transaction has been verified by the network. This happens through a process known as mining, in a proof-of-work system (e.g. Bitcoin). Once a transaction is confirmed, it cannot be reversed or double spent. The more confirmations a transaction has, the harder it becomes to perform a double spend attack.
14. **Consensus Process** is a group of peers responsible for maintaining a distributed ledger use to reach consensus on the ledger's contents.
15. **A consortium blockchain** is a blockchain where the consensus process is controlled by a pre-selected set of nodes. For example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which ten must sign every block for the block to be valid. The right to read the blockchain may be public or restricted to the participants. There are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered "partially decentralized"

16. **Cryptoanalysis** is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required to do so.
17. **Cryptocurrency** is a form of digital currency based on mathematics, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Furthermore, cryptocurrencies operate independently of a central bank.
18. **Cryptography** refers to the process of encrypting and decrypting information.
19. **A DApp** is a decentralized application that must be completely open-source, it must operate autonomously, and with no entity controlling the majority of its tokens.
20. **A DAO (Decentralized Autonomous Organization)** can be thought of as a corporation run without any human involvement under the control of an incorruptible set of business rules.
21. **The DAO** (yes, there's a difference) was a venture capital fund built on Ethereum that caused a soft and hark fork because e a venerability was exploited in the smart contract code to steal over $60M.
22. **Decryption** is the process of turning cipher-text back into plaintext.
23. **Encryption** is the process of turning a clear-text message (plaintext) into a data stream (cipher-text), which looks like a meaningless and random sequence of bits.
24. **Ether** is the native token of the Ethereum blockchain which is used to pay for transaction fees, miner rewards and other services on the network.
25. **Ethereum** is an open software platform based on blockchain technology that enables developers to write smart contracts and build and deploy decentralized applications.
26. **Ethereum Classic** is a split from an existing cryptocurrency, Ethereum after a hard fork.
27. **EVM code** is the programming language in which accounts on the Ethereum blockchain can contain code. The EVM code associated with an account is executed every time a message is sent to that account, and has the ability to read/write storage and itself send messages.
28. **A digital commodity** is a scarce, electronically transferable, intangible product, with a market value.
29. **A digital identity** is an online or networked identity adopted or claimed

in cyberspace by an individual, organization, or electronic device.

30. **Distributed ledgers** are a type of database that are spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data can be either "permissioned" or "unpermissioned" to control who can view it.
31. **Difficulty,** in Proof-of-Work mining, is how hard it is to verify blocks in a blockchain network. In the bitcoin network, the difficulty of mining adjusts verifying blocks every 2016 blocks. This is to keep block verification time at ten minutes.
32. **Double spend** refers to a scenario, in the Bitcoin network, where someone tries to send a bitcoin transaction to two different recipients at the same time. However, once a bitcoin transaction is confirmed, it makes it nearly impossible to double spend it. The more confirmations that a particular transaction has, the harder it becomes to double spend the bitcoins.
33. **Fiat currency** is any money declared by a government to be to be valid for meeting a financial obligation, like USD or EUR.
34. **A fork** is the creation of an ongoing alternative version of the blockchain, by creating two blocks simultaneously on different parts of the network. This creates two parallel blockchains, where one of the two is the winning blockchain.
35. **Gas i**s a measurement roughly equivalent to computational steps (for Ethereum). Every transaction is required to include a gas limit and a fee that it is willing to pay per gas; miners have the choice of including the transaction and collecting the fee or not. Every operation has a gas expenditure; for most operations it is ~3–10, although some expensive operations have expenditures up to 700 and a transaction itself has an expenditure of 21000.
36. **Halving:** Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block is decreased 50% every four years. This is called "halving." The final halving will take place in the year 2140.
37. **A hardfork** is a change to the blockchain protocol that makes previously invalid blocks/transactions valid, and therefore requires all users to upgrade their clients.
38. **Hashcash** is a proof-of-work system used to limit email spam and

denial-of-service attacks, and more recently has become known for its use in bitcoin (and other cryptocurrencies) as part of the mining algorithm.

39. **Hashrate** is the number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second).
40. **Initial Coin Offering (ICO)** is an event in which a new cryptocurrency sells advance tokens from its overall coinbase, in exchange for upfront capital. ICOs are frequently used for developers of a new cryptocurrency to raise capital.
41. **A ledger** is an append-only record store, where records are immutable and may hold more general information than financial records.
42. **Litecoin** is a peer-to-peer cryptocurrency based on the Scrypt proof-of-work network. Sometimes referred to as the silver of bitcoin's gold.
43. **Mining** is the process by which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies.
44. **Multi-signature (multisig) addresses** allow multiple parties to require more than one key to authorize a transaction. The needed number of signatures is agreed at the creation of the address. Multi signature addresses have a much greater resistance to theft.
45. **A node** is any computer that connects to the blockchain network.
46. **A full node** is a node that fully enforces all of the rules of the blockchain.
47. **Peer-to-peer (P2P)** refers to the decentralized interactions that happen between at least two parties in a highly interconnected network. P2P participants deal directly with each other through a single mediation point.
48. **A permissioned ledger** is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors—government departments or banks, for example—which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers.
49. **Permissioned blockchains** provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties.

50. **A private key** is a string of data that shows you have access to bitcoins in a specific wallet. Private keys can be thought of as a password; private keys must never be revealed to anyone but you, as they allow you to spend the bitcoins from your bitcoin wallet through a cryptographic signature.
51. **Proof of Authority** is a consensus mechanism in a private blockchain which essentially gives one client (or a specific number of clients) with one particular private key the right to make all of the blocks in the blockchain.
52. **Proof of Stake** is an alternative to the proof-of-work system, in which your existing stake in a cryptocurrency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.
53. **Proof of Work** is a system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work.
54. **Protocols** are sets of formal rules describing how to transmit or exchange data, especially across a network.
55. **Ripple** is a payment network built on distributed ledgers that can be used to transfer any currency. The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships.
56. **A scrypt** is an alternative proof of work system to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.
57. **SHA 256** is the cryptographic function used as the basis for bitcoin's proof of work system.
58. **Smart contracts** are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.
59. **A softfork** is a change to the bitcoin protocol wherein 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 miner's upgrading to enforce the new rules.

60. **Stream ciphers** are a method of encrypting text (cyphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.
61. **A token** is a digital identity for something that can be owned.
62. **A tokenless ledger** refers to a distributed ledger that doesn't require a native currency to operate.
63. **A transaction block** is a collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.
64. **Transaction fees** are small fees imposed on some transactions sent across the bitcoin network. The transaction fee is awarded to the miner that successfully hashes the block containing the relevant transaction.
65. **Unpermissioned ledgers** such as bitcoin have no single owner—indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies.
66. **A wallet** is a file that contains a collection of private keys.

References, Navigation and Useful Resources

In the course of putting this handbook together, several online platforms provided useful information. I will list some of them bellow;

LATEST NEWS DISCUSSIONS: https://www.facebook.com/groups/blockchaintech.co.en/

BASIC KNOWLEDGE: https://www.facebook.com/blockchain.basics/videos/

USE CASES, GUIDES, RESEARCH; WHITE P APERS: https://www.facebook.com/blockchain.basics/app/100265896690345

HACKATHON CONTESTS: https://www.facebook.com/notes/1704192179840444/Blockcha -Hackathons-&-Contests/1744256439167351/

JOBS INTERNSHIPS: https://www.facebook.com/notes/1704192179840444/Jobs-&-Internships/1741797176079944/

TRAININGS PROGRAMS: https://www.facebook.com/notes/1704192179840444/Blockch Trainings-&-Education/1737097826549879/

BIG THINK THOUGHT LEADERSHIP: https://plus.google.com/u/0/communities/100347748665926 5

GLOSSARY: https://www.facebook.com/notes/1704192179840444/Blockcha Glossary/1733001263626202/

The Ultimate Ethereum Reading List https://github.com/Scanate/EthList

The Ultimate Reading List for Blockchain, Token and Cryptocurrency Sources

http://startupmanagement.org/2017/06/06/the-ultimate-reading-list-for-blockchain-token-and-cryptocurrency-sources/

Important Disclosures

The information and opinions in this book are mine and are only intended for general information purposes and should not be regarded as a complete analysis of the subjects discussed. I do not guarantee that following the guidance in the handbook will lead to any particular outcome or result. All expressions of opinion in the book are subject to change without notice and reflect my judgment as one constantly observing the blockchain and digital currency space. I will take NO responsibility for changes in market conditions or laws or regulations and no obligation is assumed to revise this book to reflect changes, events or conditions, which occur subsequent to the date hereof. Some of the information contained in the book has been obtained from sources believed to be reliable to me and some have not been verified.

Therefore No warranty is given as to the accuracy of such information.

Created with Writer2ePub
by Luca Calcinai