An Introduction to Blockchain Technology & Cryptocurrencies

by

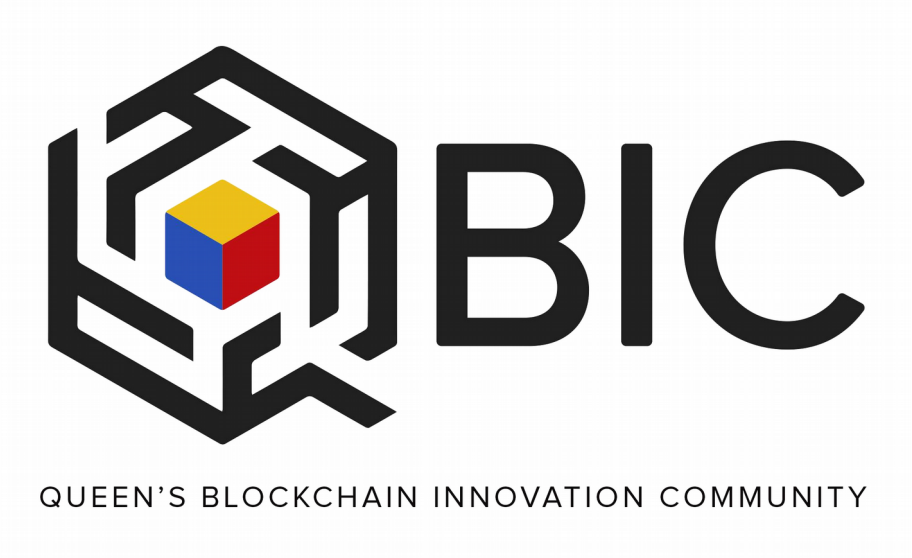


Table of contents

Chapter One: What is it?

1.1 Objective of this Primer

You've probably heard about Bitcoin in the media recently. However, you may be unfamiliar with the profoundly innovative application behind this cryptocurrency—blockchain. Blockchain is a disruptive new technology offering a decentralized network of self-compliance and regulation that challenges our current global power dynamic. This primer serves as a beginner's guide to blockchain technology and cryptocurrencies. Our focus will encompass what blockchain is and what it does, while cryptocurrencies will be touched upon briefly. The full extent of the potential impacts associated with blockchain are still undetermined. Consequently, there exists substantial misinformation regarding this technology, particularly in the media. This primer will resolve the myths surrounding blockchain and provide a thorough, yet accessible overview of the technology.

1.2 What is the Block & Chain?

A blockchain is best understood as a continuously growing list of data-containing records, called "blocks". These blocks are linked and secured using an encrypted method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Each block validates and verifies the previous block, increasing the length of the chain with each validation. The security of the chain also grows with each block added.

These blocks are represented in a publicly-distributed ledger supported by a peer-to-peer network. A system of consensus algorithms is then undertaken to ensure uniform replication across the computers and their databases involved. Blockchain's cryptographic, peer-to-peer nature renders it a secure, decentralized, and incorruptible system providing verification and consensus at a previously undeveloped level.

1.3 Public Key and Private Key - A Fundamental Concept

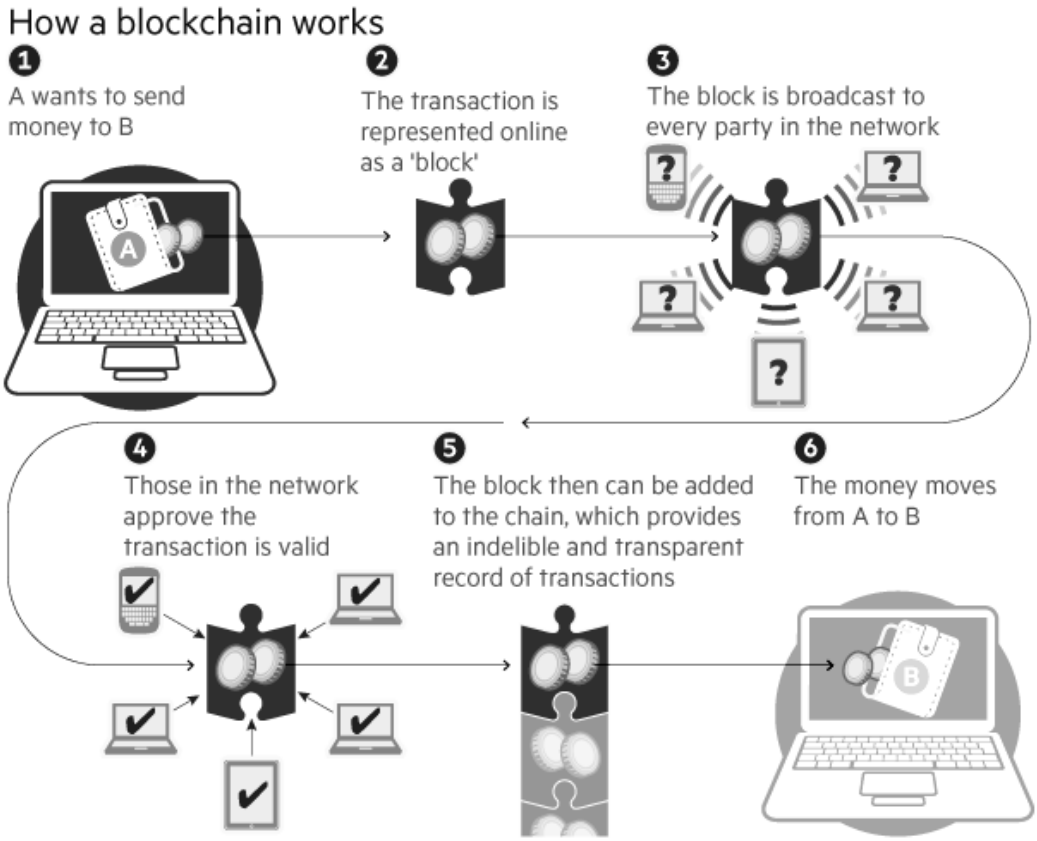
Understanding the encryption features of blockchain and cryptocurrency begins with an understanding of public and private key encryption. Access to the public key enables encryption, but does not enable the decryption of transaction information. With a cryptocurrency such as Bitcoin, using the public key enables you to view the balance of an account or use it as a receiving address. However, access to a private key is required to use funds from that account. A private key secures the funding and prevents its unauthorized movement, in other words, a private key is required to move funds. This method of encrypted securitization permeates and fuels Blockchain technology.

1.4 Bitcoin - The First chain

Here we will discuss Bitcoin as it is the first, most recognized, and simplistic example of cryptocurrency. Bitcoin is an influential global, decentralized, and borderless payment method created by the anonymous entity, Satoshi Nakamoto.

To record payment transactions in bitcoin's blockchain, you send a message created by your private key to move your bitcoin. Miners—computer users connected to the bitcoin network over the internet, verify and confirm these transactions. Data is then placed into the next block of transactions. The new encrypted block records your transaction, i.e. that you have sent a given amount in Bitcoin. A recipient receives, and now has the sent-amount of Bitcoin stored in their account.

A primary innovation of Bitcoin, as well as the source of its decentralized nature, is the use of miners. Miners are paid a small amount of bitcoin for each block they confirm and add to the network. As a result of the immense computational power required for mining, Bitcoin's network, likewise, requires massive amounts of power. With each confirmation of increasingly complex encrypted transactions, miners require more electricity and computational power at their disposal. The more a Bitcoin is worth, the more individuals are willing to mine for them. Power usage is thereby connected to Bitcoin price. These factors all converge, generating a system based on keys and encryption. This system can be anonymous or identifiable, while being run by a peer to peer network sans third parties. In place of the regulatory structure imposed by banks and other third parties, Bitcoin utilizes an agreement computer code.



Source: Halpern Financial

1.5 Innovative Benefits Of The Next Internet Technology

1.51 Efficiency and Reliability

Blockchain has the potential to make financial transactions and the exchange of information more efficient, reliable, private and secure. Prior to blockchain, moving money or assets, was only possible through a centralized body. For example, if I wanted to send money from Person A to Person B, my options would be through a bank, credit card, Paypal etc. These centralized bodies have drawbacks, because they are often inefficient, exclude parties, and come with exorbitant transaction fees.

For families who wish to send money to relatives in another country, transactions may take days to confirm, while an average fee of 9% significantly reduces the final amount received. However, Blockchain eliminates the requirement of a bank, confirms payment much quicker, and with significantly lower fees.

Blockchain's automated-trust mechanism enables this, alleviating the necessity of an intermediary. Instead, coding and cryptography performs the traditional functions of a bank, which is ensuring a successful transaction between two parties. Banks can no longer monopolize on the movement of currency, nor are there restrictions of movement based on accepted geographical borders. Many blockchain-encrypted currencies are already faster, and more reliable than the banking system, particularly when moving money internationally.

1.52 Immutability

Blockchains encryption method (or hash see section 8), is a function that converts an input of letters and numbers into an encrypted output of a fixed length, creates an unalterable ledger that allows anyone to see the entire history of all transactions. Therefore, it is impossible to forge transactions, exploit, or manipulate the system, which would require either hacking, or owning 51% or more of the global hashing power for that blockchain. A hacker would have to take control of 51% of the millions of computers on the blockchain network. A task that is unfeasible due to the time commitment and economic resources required.

1.53 Democratic

If 51% of the system agrees on a ledger, that agreement is the ledger—making Blockchain a functioning democracy of sorts. Blockchain is consensus building on a massive scale, which is suitable given that the technology is built around consensus algorithms. A lack of central authority means that there is no single source of corruption or control in the system. Across some applications of blockchain, such as the original form of Bitcoin, any change in the underlying code required complete consensus from 51% of investors. This is similar to how firms require the consensus from a board of directors before changes are made.

In the case of Bitcoin, there was no consensus among investors over proposed changes, consequently, a portion of Bitcoin seperated and formed another cryptocurrency, Bitcoin Cash. Ultimately, it is crucial to understand that no one individual regulates a blockchain, the system is run by an entire network, operating on a vast network of computers.

1.54 Borderless

An advantage of blockchain is its capacity to transcend borders. The blockchain is only limited by the reach of the internet, which could usher in a global market with no obstacles to participation. This increases the potential for growth and diversification in our economy. Since these transactions are digitally-based and borderless, individuals and companies are able to reach the entire global market. It has also become common for people to seek funding on the chain rather than the stock market for their start-up company cash. By engaging in Initial Coin Offerings (ICO's), as opposed to stock a offerings, companies are able to raise funds in unprecedented ways. Blockchain technology often operates without government oversights due to its borderless nature as well. Limited government intervention has several benefits, including enhanced efficiency due to less bureaucratic red tape.

Chapter two: What can it do?

To ascertain whether blockchain is applicable to to an industry, technology, problem solving, or more, knowledge of these four perspectives is necessary.

2.1 Privacy & Security - The Secure Internet

Privacy and security has been difficult to maintain on the internet. However, one's online-identity and information can be stored on the blockchain at a public address, secured by your own private key or password. Blockchain is a technology that will allow citizens to take control of, and protect their data, potentially ending the corporate practice of accumulating and selling customer data.

Examples: Recent security breaches such as the Equifax hack, where millions of identities and financial data were stolen. Spam control, where someone's email could be linked to multiple publics keys. They would know who shared your email and remove mailing consent instantly. Same premise could be used to sharing and owning games, movie, music, even patents, any kind of intellectual ownership.

Blockchain offers a viable method to store and protect data. Cyber attacks would face monumental barriers in the future as databases and critical information could be encrypted using blockchain technology. This is the fundamental promise of all blockchain - the secure internet.

2.2 Directories & Databases - Storing Information In A New Way

Blockchain is essentially a database. The nature of the technology ensures safe and private storing of data, which has many benefits. One example is personal medical records. Imagine if the same medical record was shared with multiple hospitals. These records couldn't be decrypted without the agreement from the hospitals. Your personal data is kept safe and private. Now imagine each part of the record is encrypted differently. Hospital researchers are empowered and incentivized to search for a record of people with one type of illness, in one part of the hospital, with no personal information included. There is already a start-up planning to do the same with DNA records. Government are also experiment titles deeds citizenship, passports, employment and tax record. That was not an exhaustive list. Any important database can make use of the reliable, secure, and decentralized power of blockchain.

2.3 Assets & Currency - Cryptocurrencies

More can, has been, and will be written on this part of blockchain than this primer could ever illuminate. Currencies connects needs with supply. It is often said, Blockchain allows for the "brings consumer and producer closer together". It does this in a way old currency systems could not.

Imagine an aspiring musicians could trade their music for cash, and you the supporter gets a token. Soon, the muscain takes off, and the only way to their concert is with the tokens you have. You can sell them, trade them, attend or even hold. You have the choice, in a simpler, safer, and more transferable way than ever before. Many see this as the beginning of a new decentralized sharing economy. In mid 2017 over a thousand cryptocurrencies were in circulation. The industry is bloated with hundreds Initial coin offerings (ICO's). Blockchain has revolutionized crowdfunding creating new and yet unstabilized monetary system. Its called "The Token Economy"

This monetary system contain all of blockchains previously listed advantages. It is mostly out of government control. Most investors are either throwing in any funds they can find, or terrified of this new economics system. Only time will tell when and how these system will enter our everyday financial lives.

Altcoins Examples

- **Ripple** - Designed for big banks, to be their new payment and settlement network.
- **Bitcoin Cash** - Bitcoin fork with more developer support, allows for larger file-size blocks, and the possibility of smart contracts.
- **Dash** - Short for digital cash, a decentralized autonomous organization (DAO) with a focus on privacy, scalability and instant transaction confirmations.
- **Monero and Zcash** - More anonymous and private cryptocurrency.

- **Tether** - A cryptocurrency exchangeable for one U.S. dollar. Its value is always nearly exactly one U.S. dollar, yet has the advantages of trading as a cryptocurrency.
- **IOTA** - Not supported via blockchain, uses an alternative structure called the DAG/tangle. Look for it in the future.

2.4 Smart Contracts - Next Generation of Function

So now we have a secure database system. One that can revolutionize multiple internet industries, and our financial world. Imagine now that this database could execute programs like computer. These automated operation are called smart contracts. They use information like a secure digital identity, other forms of information, currencency, or almost always work without human intervention. Major examples of the smart contract platforms Ethereum, Neo, and Cardano, The limits of this technology just being touched on now.

- **DApps (Decentralized Applications)** Applications built to run on the blockchain network to leveraging advantages of blockchain tech. Paying with the smart contracts token is the costs of running or using these apps on the network.
- **ICO (Initial Coin Offering)** Most modern ICO's are actually on a smart contract platform You can buy and sell with the already existing platform. This way not every new ICO has to set up the own blockchain system. They just pick a smart contract platform instead. Very little set-up, yet all the blockchain advantages retained. Transactions our paid by paying for a smart contract.
- **DAO (Decentralized Autonomous Organization)** — an organizational structure that is run using smart contracts code, assigning voting rights to members via token ownership system.

Many theorize financial derivatives, conditional sale of patent and information, land deeds and titles, even democratic and institutional structures will make use this technology. The Canadian national research council is already experiment is already with use of ethereum to control costs and spending on projects. The other example E-estonia, a project to digitize an entire nation, could be put down as a use can in itself. It has Blockchain based voting, citizenships right/status and is taking this technology as far as it can

With this chapter we hope the reader see blockchain as more than just one thing. We hope the reader see it as a dynamic and technological tool. One, which gives us chance to better organize the world's data, finances, and institutions.

Chapter Three: What should I take away from this?

3.1 Where is it All Headed?

Skepticism of Bitcoin and other cryptocurrencies can be overblown. Furthermore, skepticism of Bitcoin does not justify skepticism towards blockchain as a technology. Blockchain isn't simply Bitcoin, it also powers Ethereum, Ripple, a myriad of startups, and peoples' lives. Major companies such as HP, Intel, IBM, Microsoft, Google, Goldman Sachs, J.P. Morgan, and Canada's five biggest banks are all investing heavily in this technology and its ideas. They are using their money, time, and effort for good reason. We are not trying trying to hype blockchain beyond measure. We obviously are not saying it will just go away and be forgotten. It only needs to be understood: like the internet, and other revolutionary technological innovations before it, Blockchain is here, and here to stay. The Ideas and concepts underlying it are changing our world. Right now and into the future.

3.2 What is QBIC?

The Queen's Blockchain Innovation Community was founded in the fall of 2017 and consists of students across various faculties, including economics, philosophy, and computer engineering. Our purpose is to discuss topics and ideas central to blockchain. We also promote user adoption, research, and reporting on blockchain here at Queen's University. QBIC seeks to advocate and foster awareness of the importance of blockchain through organizing non-profit seminars, and linking student and associated talent with private partners. This non-profit group and its projects are sustained solely by the passion and curiosity of a volunteer collective. If you are as passionate about the possibilities of blockchain technology as we are and would like to get involved, or you have any questions please reach out so that we can work with each other in a collaborative capacity. Lets foster awareness together.

Bitcoin

Ethereum

BTC: 3EHMJ96ygaWEW9BvmjhuNXfrqy5b2siV9d

ETH: 0x455e5F4Cf3C00F1bDb3328d8Db0bD5FFc2b5a692

3.3 Local Blockchain Technologies

BitSwift is an Internet technology company specializing in Blockchain technical support, and consulting. Bitswift offers expertise on blockchain-based currency, inventory management, and security systems. The company essentially advocates for the use of cryptocurrency in everyday trade. They have a passion for helping small business make of cryptocurrencies and more.

Sparc is an emerging player that understands the supply-and-demand problem. Most of the world's computing power is uncultivated. Sparc has created a system based on existing technology to utilize untapped computer power. It can run on almost any modern machine. You rent out your computer and get paid in sparc tokens (cryptocurrency). Billions of computers around the world sit idle. All while everyone from gamers to researchers are building bigger and more powerful machines to run their systems. Sparc intends to bridge these two areas.

3.4 Conclusion

Blockchain is a world changing, adaptive, secure internet database technology, consisting of local and global players. Its power is not linked to a single application, but a family of ideas and uses. The technology will strengthen the consumer-producer relationship by rendering intermediaries obsolete, as well as simplify transactions and trade. Blockchain redefines ownership, agreements, and contracting. Like all new technologies, blockchain is disruptive. Expect institutions to appear, disappear and change because of it.

In the city of Kingston, Ontario, which is home to two emerging blockchain-related companies, BitSwift and Sparc, as well as population of 150,000, blockchain has a real presence. It may not be apart of your everyday life just yet, but blockchain is growing here and all over the world. You will see it more and more. Blockchain has the potential to create a better future for everyone, we hope you will join us in helping create this future.

Sincerely,

QBIC

V 1.0 Lead by James Hazlett & co-authored by Josh Malm, Oliver Philpott, Michael Krakovsky, Nickolas Chan and Kris Jones.

4# - Appendix

4.1 Glossary

4.1.1 Blocks

Data-containing records, linked and secured using an encrypted method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it

4.1.2 Public Key

Access to the public key enables encryption, but does not enable the decryption of transaction information.

4.1.3 Private Key

A private key secures the funding and prevents its unauthorized movement, in other words, a private key is required to move funds.

4.1.4 Encryption

The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

4.1.5 Ledger

Collection of an entire group of similar accounts in double-entry bookkeeping. Also called book of final entry, a ledger records classified and summarized financial information from journals (the 'books of first entry') as debits and credits, and shows their current balances.

4.1.6 Initial Coin Offerings

An ICO is a fundraising tool that trades future cryptocoins in exchange for cryptocurrencies of immediate, liquid value.

4.2 Technical terms

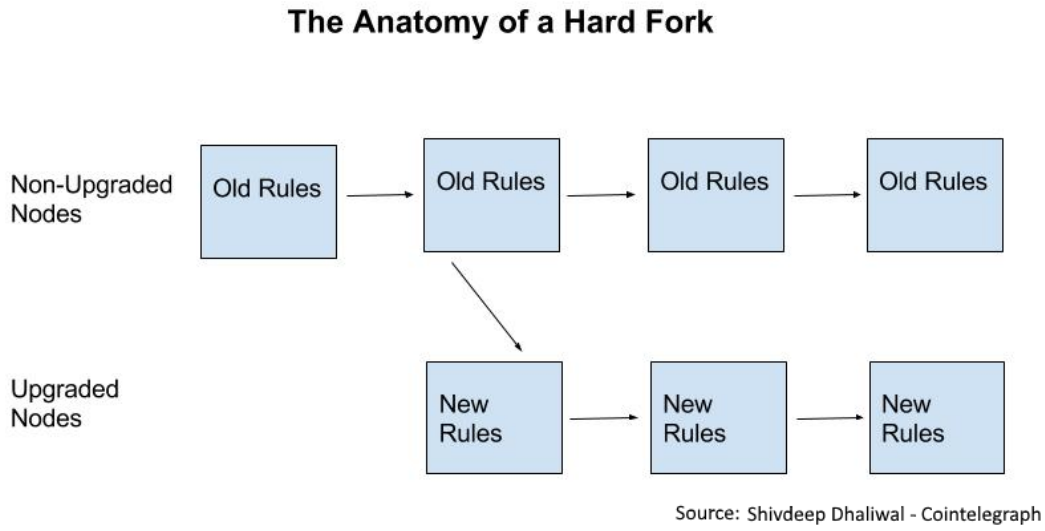
4.2.1 Block Height

Block Height alludes to the number of Blocks connected in a Blockchain. For example a Block Height of 0 would be the first block (also known as the genesis block) in a blockchain.

4.2.2 Hard Fork

A hard fork, or forking, is a type of blockchain evolution. There are 3 main types of forking protocols. The first occurs when two miners mine two different blocks at the same time, temporarily splitting the blockchain into 2 different versions called “Orphan blocks". This type of forking is quickly rectified and is a natural part of the blockchain.

The second type of forking occurs miners do not simultaneously update as the system does, resulting in two chains at a “fork”. The third occurs when a disagreement among developers about the progress of the blockchain results in a separation, and creation of 2 distinct blockchains. Examples are Ethereum Classic and Ethereum, and the many bitcoin forks (e.g. Bitcoin Cash, Bitcoin Gold, and Bitcoin Diamond).



4.2.3 Mining

Creating a new block requires running, and validating, a block through a HASH. This is a computer-intensive process. For your work, you accept a cryptocurrency reward. Mining is one of the biggest innovations of Bitcoin, as it rewards the decentralized system. Few cryptocurrencies function without miners and they almost all have a governing authority of some kind (e.g. IOTA, Ripple).

4.2.4 Confirmation

Bitcoin blocks are made every ten minutes. This means you need to wait ten minutes for anything to go through. On some exchanges multiple block confirmations are required prior to the confirmation of a transaction.

4.2.5 Proof of Work (PoW)

Cryptocurrency blocks must be hashed. An added variable, timestamping blocks, and transactions all must be validated. Since Hashing is difficult and takes considerable computational power, a hashingblock is considered proof of work.

4.2.6 Proof of Stake (PoS)

Proof of stake is an alternative way to determine consensus similar to proof of work (PoW). The process in PoS is called forging or minting instead of mining. While there is still decentralized power to confirm transactions, the “minter” that adds each block is chosen as a result of holding their stake (possession of currency or a token). The minters still process the changes and retain transaction fees, however there is typically no block reward in a PoS system. The main goal of proof of stake is to improve the efficiency of blockchains. There are several examples currently in use, such as NEO, Decred, PIVX.

4.2.7 *Application Specific Integrated Circuit (ASIC)*

Otherwise known as Application Specific Integrated Circuits. These are computer chips designed to accomplish a single task, namely mining cryptocurrencies. Bitcoin miner, Bitmain has a plethora of these chips, entitling them to over 25% of the computational power on the Blockchain. Since Bitcoin employs consensus algorithms, this single mining company's vote is worth 25%, in terms of determining the future of bitcoin.

4.2.8 *Hash*

The Hash is a generic term referring to a wide array of cryptographic algorithms. Usually they turn an input, a string of letters, into an output. With Bitcoin, every ten minutes a letter is added to this sequence, making a new output for that block and time stamping that block. The next block begins with a reference to the previous hash. This way every hash is linked, timestamped and validated by the previous block in the chain. To break any new block by adding fake transaction, you need to break every previous block at once. Bitcoin uses Secure Hashing Algorithm (SHA) 256. Right now you cannot break SHA-256. it has "**1157920892373161954235709850086879078532699846656405640394575840079131296396**" Combinations. Checking each one is impossible.

Final note: Quantum computer will likely lead to massive changes in how hashes work. They can crack SHA 256. Even though they are not here yet, many current generation blockchain are already being built and released with quantum resistant ledgers.