Breaking Down Blockchain:

The Science Behind the Revolutionary Technology

AN INTRODUCTION TO BLOCKCHAIN

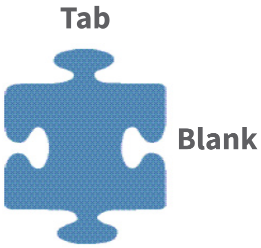
Blockchain is a revolutionary technology developed in 2008 as a database for storing information in a way that makes it difficult or impossible to change, hack, or intercept. Its many applications include recording transactions, sending payments, and sharing data. Just as the internet revolutionized multiple industries and ushered in a new digital age, blockchain has the potential to have a similarly profound impact on the economy.

As its name suggests, blockchain can be understood as **blocks** of information that are **hashed** together with **digital signatures** to form a **chain** of encrypted records. Blocks are accessed, hashed, and stored via **nodes**, or access points, across a **distributed peer-to-peer network**. The revolutionary characteristics of blockchain are its **distribution, immutability, and incorruptibility.**

BLOCKS

A **block** is essentially a digital record that stores information. Just as a puzzle piece depicts part of an image, a block records digital information. A block can record virtually any type of information in digital format. Whether it be a financial transaction, a legal contract, or a medical record, blocks have limitless applications.

The concept of digital information is not new. However, the manner in which blockchain records, distributes, and accesses information is what is revolutionary.



HASHING AND DIGITAL SIGNATURES

Hashing is the process that binds blocks of information together. Just as tabs and blanks interlock different puzzle pieces, a string of hashes holds blocks of digital information together. Just as puzzle pieces interlock to form one continuous image, hashing creates one continuous and recognizable chain of information. And just as you cannot take a piece of a different puzzle to connect with an existing puzzle, digital signatures ensure that the origin and authenticity of new data can be verified.

The combination of hashing and digital signatures is the most innovative and central concept behind blockchain. In a word, hashing and digital signatures are what enable a blockchain to be both immutable and incorruptible, while being universally verifiable across a distributed network. While hashing and digital signatures serve multiple functions in blockchain technology, we will focus on three of their most crucial functions: the addition and conversion of data into a universal format, the verification of the origin and authenticity of new data, and the protection of the entire blockchain of data.

CONVERTING AND ADDING DATA

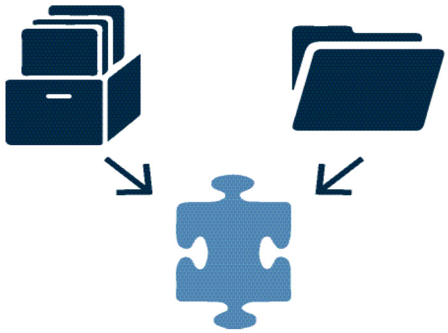
Hashing converts data of any size and any format into a universally recognizable format called a **hash**. To use the puzzle analogy, hashing converts information into a puzzle piece, which can then be connected to other interlocking puzzle pieces in the existing blockchain.

In more technical terms, hashing generates a fixed output regardless of the size of the input. A single transaction or a ledger with a thousand transactions produce a string of letters and numbers with the exact same finite length, known as a hash:

(Single Transaction = A0680C04C4EB53884BE77B4E10677F2B)
(1,000 Transactions = A0680C04C4EB53884BE77B4E10677F2B)

The hashing process links together a **chain** of blocks, thus the term "blockchain." To use the puzzle analogy, the hashing process both converts data into a puzzle piece shape and interlocks it with the preceding puzzle pieces.

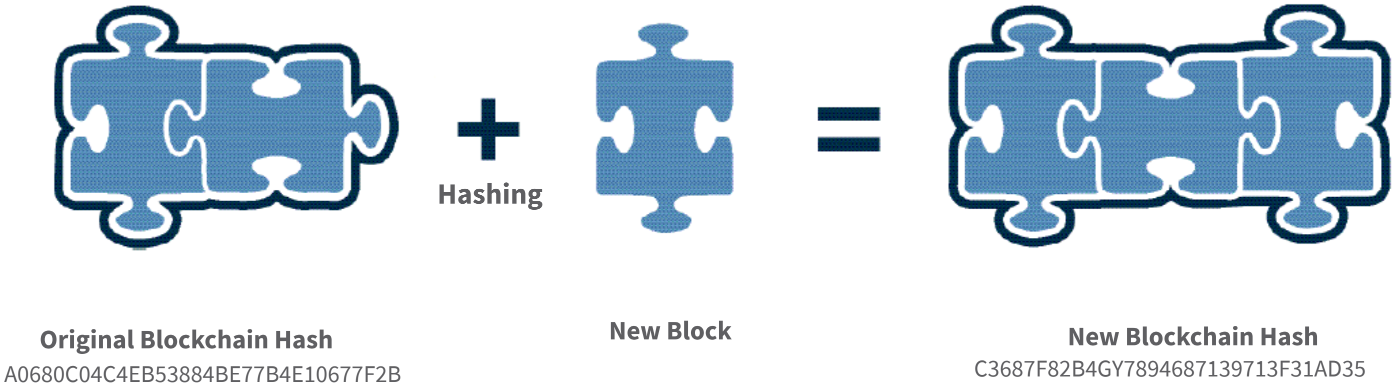
Converting Data



In more technical terms, new data is added to the existing blockchain by hashing it together with the entire preexisting blockchain. The output is an entirely new hash which represents the new state of the blockchain.

In order to hash information together, a computer must solve a complex problem. The computer must input different variables until the problem is solved. To use the puzzle analogy, this process is akin to rotating a puzzle piece until it fits with the preceding puzzle pieces (if each puzzle piece had an infinite number of unique tabs and blanks). Individuals who successfully hash new information to the existing blockchain are rewarded with a fee paid in Bitcoin, a digital cryptocurrency.

Adding Data


+
Hashing
=
Original Blockchain Hash
A0680C04C4EB53884BE77B4E10677F2B
New Block
New Blockchain Hash
C3687F82B4GY7894687139713F31AD35

VERIFYING DATA

Digital signatures verify the origin and authenticity of new data when it is added to the blockchain. To use the puzzle analogy, this process validates that each new puzzle piece came from the same puzzle box and prevents puzzle pieces from different puzzle boxes from being added to the existing puzzle. In a word, digital signatures ensure that information has not been altered before it is added to the blockchain.

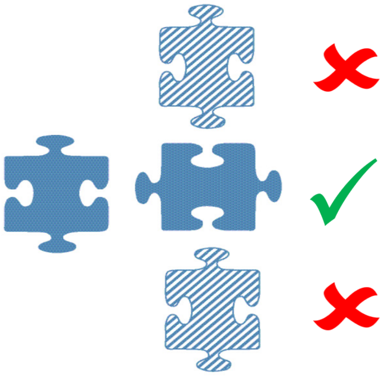
In more technical terms, a ‘private key’ is used to encrypt data via a cryptographic function. This produces a unique digital signature which verifies where the data came from and whether it has been altered. However, as with any lock, its effectiveness is dependent upon the security of the key. If a private key is compromised, it can compromise the security of the digital signature.

PROTECTING DATA

In combination with digital signatures, hashes protect the integrity of the entire blockchain. In addition to connecting each block of information, the hashing process also indicates whether preexisting information in the blockchain has been altered. Just as puzzle pieces interlock to form one continuous image, hashing creates one continuous and recognizable chain of information.

In more technical terms, hashing generates an entirely new hash anytime data is modified. To use the previous example, modifying data from “1,000 transactions” to “1,001 transactions” will generate a completely different hash. To use the puzzle analogy, if a puzzle piece is removed and replaced with a different puzzle piece in an interlocked chain, it will no longer depict the same continuous image. The same holds true for a blockchain. If data is removed or replaced, the new hash will no longer match the previous hash. This process allows altered data to become instantly recognizable. In combination with its distributed nature, hashing enables blockchain to theoretically be both **incorruptible** and **immutable**.

Hashing



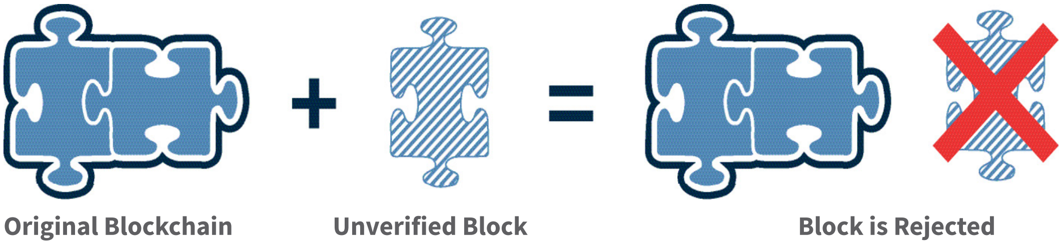
(1,000 Transactions = A0680C04C4EB53884BE77B4E10677F2B)
(1,001 Transactions = C3960F32D5FF87923AC64E4E10472A3A)

DISTRIBUTED PEER-TO-PEER NETWORK

The entire blockchain is hosted on a distributed peer-to-peer network, which is accessible via a network of nodes, or access points. As its name suggests, a peer-to-peer network is a network that connects peers directly, which eliminates the need for an intermediary. In the case of blockchain, this network is distributed across multiple nodes, which all host identical copies of the current blockchain. This is in contrast to a ‘centralized’ (or ‘decentralized’) network, where data is hosted on only one (or a handful) of access point(s).

The blockchain is hosted simultaneously on all access points and updated instantaneously across the entire network. Every addition to the blockchain is visible to all access points at all times. To use the puzzle analogy, a distributed peer-to-peer network depicts the puzzle in its current state across the entire network. Anytime a puzzle piece is added, it is instantly reflected across the entire network.

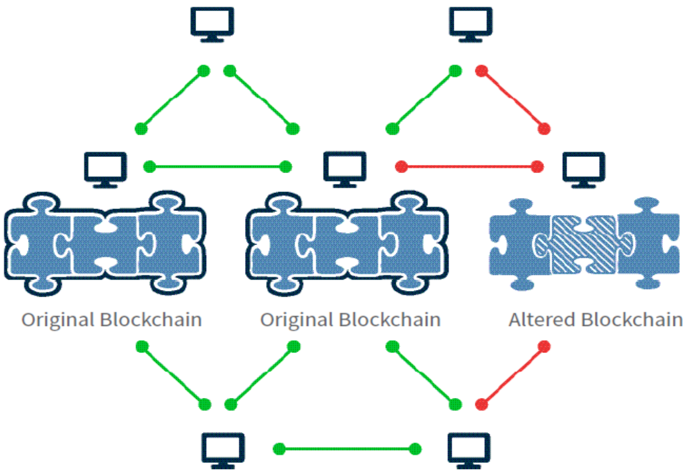
Verifying Data



Due to the fact that the blockchain is not stored within one central access point, this vast distribution of information across multiple systems essentially renders data alteration or hacking ineffective and virtually impossible. If an individual attempts to alter the blockchain via a network node, it will generate a different hash that will not match the hashes hosted on all the other network nodes.

Whereas a centralized network only has a single record of data to which all other nodes refer, a distributed network can readily identify information which has been altered and does not match the existing information on the network. This notion of distributed information is similar to diversification within a stock portfolio. Just as an investor inherently assumes more risk by concentrating all his capital in a single stock, a network assumes more risk by concentrating all of its information in a single access point. On the other hand, just as an investor reduces his risk by distributing his capital amongst multiple assets, a network reduces its risk by distributing information across multiple access points. This is arguably the most revolutionary aspect of blockchain.

Altering Data in a Distributed Chain



POTENTIAL APPLICATIONS

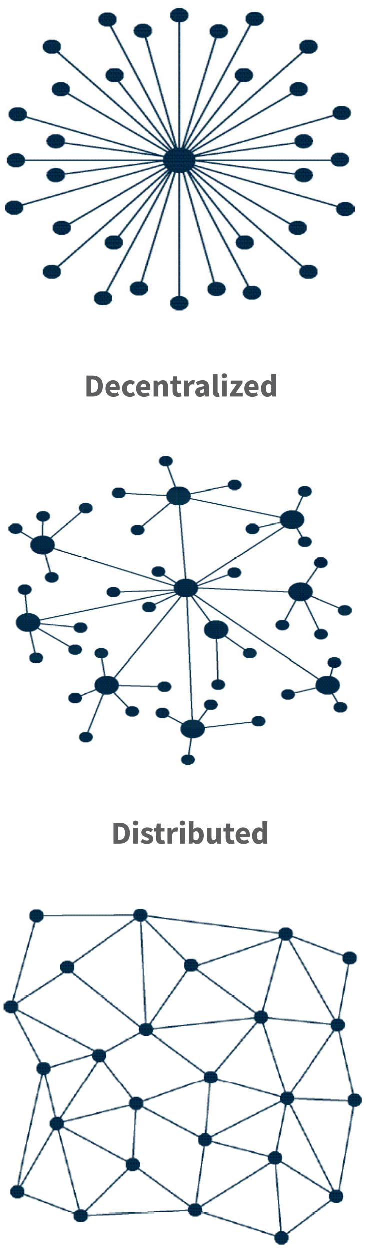
With an infinite number of possible applications in numerous industries, blockchain technology has the potential to revolutionize the global economy on a scale not seen since the advent of the internet. Just as the internet revolution fundamentally changed nearly every imaginable aspect of modern life and created entirely new industries, the size and scope of the blockchain revolution is similarly profound. However, as with any emerging technology, the principal benefactors of blockchain have yet to be determined.

Whether it be validating the authenticity of ingredients in an international pharmaceutical supply chain, expediting financial audits with a far greater degree of accuracy, or verifying the identities of voters in democratic elections and increasing voter turnout, it would seem that the potential applications of blockchain technology are only limited by the human imagination.

Centralized

Decentralized

Distributed



All content written and assembled by the Investment Strategy Group.

CRYPTOCURRENCY DISCLOSURES

Prior to making an investment decision, please consult with your financial advisor about your individual situation. The prominent underlying risk of using bitcoin as a medium of exchange is that it is not authorized or regulated by any central bank. Bitcoin issuers are not registered with the SEC, and the bitcoin marketplace is currently unregulated. Bitcoin and other cryptocurrencies are a very speculative investment and involves a high degree of risk. Investors must have the financial ability, sophistication/experience and willingness to bear the risks of an investment, and a potential total loss of their investment. Securities that have been classified as Bitcoin-related cannot be purchased or deposited in Raymond James client accounts.

REGULATORY BACKGROUND | Financial Industry Regulatory Authority ("FINRA") and the Securities and Exchange Commission ("SEC") have issued multiple warnings to investors regarding the risks associated with Bitcoin and other cryptocurrency. New products and/or technology, such as Bitcoin and other cryptocurrency, are typically considered high-risk investment opportunities as they commonly are targeted by fraudsters who manipulate the market with artificial promotional scams. As of March 2017, the SEC rejected multiple applications from fund companies seeking to create and list a cryptocurrency Exchange-Traded Product ("ETP") due to the highly unregulated nature of the cryptocurrency marketplace. The biggest risk factors surrounding Bitcoin (and other cryptocurrency) issuers include that they are not registered with the SEC (or local country regulator) and can be exploited by criminals for money laundering/terrorist financing making the source of funds difficult to follow and verify.

RJF CRYPTOCURRENCY SECURITY DEFINITION | A Cryptocurrency Security is one associated with a public company and/or issuer that is affiliated with the digital currency marketplaces by processing transactions or facilitating payment services. Additionally, other aspects of the relationship to cryptocurrency like Bitcoin may include, but are not limited to, the following:

1. Indexed to the underlying price movement of cryptocurrency

2. Cryptocurrency Mining

3. Cryptocurrency Escrow Services

4. Cryptocurrency Business Operations

5. Cryptocurrency Start-ups

Of note, the definition of a Cryptocurrency Security does not include public companies who accept bitcoin or other cryptocurrency as payment for goods and services (e.g. Expedia, Overstock.com and Dish Networks).

RJF POLICY | Effective April 10, 2017 and as unanimously approved in the March 29, 2017 Anti-Money Laundering Oversight Committee ("AMLOC") meeting, RJF will prohibit the trading, receipt of (as applicable) and/or deposit of known Cryptocurrency Securities that are not listed on a U.S. National or Internationally Approved Securites Exchange. This policy applies to all RJF business units and subsidiaries, both domestic and international. Any exception or exemption to this policy must be approved and documented in accordance to the requirements set forth in the RJF HRS Policy. A list of known Bitcoin and Cryptocurrency Securities will be distributed with this memo and included within the master list of prohibited securities owned by the RJF Securities Review Unit.

ADDITIONAL DISCLOSURES | Views expressed in this newsletter are the current opinion of the author, but not necessarily those of Raymond James & Associates or your financial advisor. The author's opinions are subject to change without notice. Information contained in this report was received from sources believed to be reliable, but accuracy is not guaranteed. Past performance is not indicative of future results. Investing always involves risk and you may incur a profit or loss. No investment strategy can guarantee success.

Not FDIC or NCUA Insured • No Bank Guarantee • May Lose Value

RAYMOND JAMES®

INTERNATIONAL HEADQUARTERS: THE RAYMOND JAMES FINANCIAL CENTER
880 CARILLON PARKWAY, ST. PETERSBURG, FL 33716

Investment products are: not deposits, not FDIC/NCUA insured, not insured by any government agency, not bank guaranteed, subject to risk and may lose value.