The BlockChain Bible

Original http://www.digital-astronauts.com/the-blockchain-bible/

Format

Blockchain is the foundation of Bitcoin and cryptocurrency, a trend that has been getting huge levels of attention recently.

Whether or not Bitcoin is a worthwhile investment remains to be seen, but for those who bought Bitcoin in the beginning, their investment has yielded insane dividends.

Bitcoin was founded in 2009, but it wasn’t until a year and a half later that man named Laszlo Hanyecz was the first person to spend Bitcoins in a financial transaction.

Lazlo traded someone 10,000 bitcoins to for two papa john’s pizzas, a transaction of 41$.

Today, the Bitcoins spent to relieve his craving for take-and-bake, are valued at 150 Million.

The reason that Bitcoin’s value has increased in such a dramatic way?

Though many forces are causing Bitcoin’s value to rise, such as shifting attitudes of large investors and Bitcoin fans refusing to sell bitcoin to drive up the price above 1M per-coin, none of the success of Bitcoin would be possible without blockchain.

Blockchain for Beginners

Before we cover more applications of the blockchain technology behind Bitcoin, here are the basics for those who are less familiar with blockchain.

What is Blockchain?

A blockchain is a data set known as a “distributed ledger” that creates connections between different data points, called blocks, in a chain that is unbreakable and unalterable.

Blocks are linked by “hash pointers,” which connect each block and encrypt the information within blocks.

Hash Pointer:

Hash: Cryptographic hash of information (ie. a Bitcoin transaction).

+

Pointer: A link to where the hashed data is stored.

Stored in this encrypted format, the data in a blockchain is accessible but unalterable, a perfect record of whatever you happen to be recording.

Essentially, blockchains are massive spreadsheets, and the entries in this spreadsheet range from the transactions conducted using a Bitcoin, to the location of a product being shipped, to the policy information of insurance holders.

What is Blockchain technology?

Blockchain technology is technology that uses blockchain to achieve or support its functionality. Technology using blockchain is poised to become the new standard for many business processes and for data security, data storage and data sharing needs of companies.

Examples of Blockchain Applications

Here are just a few examples of companies that are applying blockchain to innovate in established industries:

- **Providence** – Tracks Yellowfin Tuna from catch to plate with blockchain.
- **Symbiont** – Blockchain applications for enterprises to manage loans, the distribution of index data, private equity and crowdfunding and ensure data accuracy/security.
- **Kik** – A messenger platform that uses blockchain for message threads.
- **Shapeshift** – An online exchange for different cryptocurrencies, (ie: bitcoin into z-cash, ether, etc.).

- **IBM** – A wide variety of blockchain applications, from verifying food safety and tracking commodities through supply chains to clinical trial management and data security.

What is Blockchain Wallet?

Blockchain wallets are applications used to save the addresses of blockchain currencies and conduct financial transactions with Bitcoins or other cryptocurrencies.

What is Blockchain Used for?

Blockchain has proven to be useful or even revolutionary in a number of industries, from healthcare to finance, from insurance to education.

Here’ s how blockchain is changing the way that business is done in established industries:

What is Blockchain in Insurance?

Using Blockchain for data storage in the insurance industry may become the new standard before long.

The data security offered by blockchain, along with the ability to eliminate fraud and redundancies in policy information, make blockchain a natural fit for the insurance industry.

Blockchain also allows for “smart contracts” that can automatically approve or deny insurance policy claims, based on whether or not claim data meets the conditions of the smart contract.

What is Blockchain in Finance/Banking?

In finance and banking, blockchain has the ability to manage a huge number of processes and is speculated to have sweeping applications throughout the finance and banking industries.

Here’ s an excellent take on blockchain in finance from the Harvard business Review:

“Money, equities, bonds, titles, deeds, contracts, and virtually all other kinds of assets can be moved and stored securely, privately, and from peer to peer, because trust is established not by powerful intermediaries like banks and governments, but by network consensus, cryptography, collaboration, and clever code.”

Additionally, as cryptocurrency gains popularity and major financial powers like China take steps towards embracing digital currency, blockchain may revolutionize our financial system and may remove the need for as many intermediary companies involved in finance and banking.

What is Blockchain in Healthcare?

Blockchain in healthcare helps to manage data and automate processes in an industry where accuracy is literally a matter of life or death.

Medical error is one of the most common causes of death in the US, and storing patient records in a distributed ledger reduces redundancies and errors that lead to these deaths. Blockchain also allows for more accurate tracking of pharmaceutical medication, which will both help patients and help to reduce the diversion of opiates into illegal markets.

What is Blockchain in Supply Chain / Logistics?

In the supply chain and logistics industries, blockchain makes it much easier to track the location of commodities as they are created, packaged and shipped to different points along the way to store shelves.

Smart contracts will allow payments and authorizations to be triggered by the GPS location of packages as they are shipped, helping to increase efficiency in the 1.5 trillion dollar industry.

What is Blockchain in Real Estate?

In real estate, blockchain is helping to increase the efficiency of property transactions by decreasing the time it takes to verify an individual’ s financial information and improving transparency in the industry.

Blockchain would also help to make forged ownership documents and fake rental listing scams impossible, by having all transactions related to a property being incorruptibly while in a blockchain.

What is Blockchain in Education?

In education, blockchain could help to standardize the authentication of certificates issued from learning institutions.

Blockchain will also help to ensure that the credentials of all educators are valid and eliminate redundancy and error in student performance data.

What is Blockchain in Marketing?

Marketing applications of blockchain are diverse, and this industry will improve accuracy when targeting consumers as well as increasing data transparency for these consumers.

Blockchain can be used to ensure that people are not over-exposed to particular ads or even to automatically pay people for using their data. It can also be used to verify that followers are people, not bots and to guarantee the legitimacy of sponsored contests, ensuring that only one vote is given to each participant.

What is Blockchain for Business?

Blockchain has a great number of applications for businesses of all kinds, from improving the accuracy and transparency of records to eliminating time consuming back of office processes.

The applications of blockchain in business are still being discovered and optimized, and we may see a widespread adoption of this technology across industries in the coming years.

Why Blockchain Matters?

Blockchain matters because, for now, it is one of the most secure and practical ways to store data sets, especially when these data sets are used by multiple parties for multiple purposes.

Early adopters of blockchain applications are already reaping the benefits of improved data visibility, integrity and security, and, as use of blockchain proliferates, more and more industries will grow to depend on this technology.

What is Blockchain Mining?

Blockchain mining is most commonly applied in Bitcoin mining.

Bitcoin Mining is where individual “miners” solve math problems created by mining computers to add a series of bitcoin transactions to the public record of bitcoin transactions.

Here’s a detailed explanation of Bitcoin Mining from The Economist:

“Every ten minutes or so mining computers collect a few hundred pending bitcoin transactions (a “block”) and turn them into a mathematical puzzle. The first miner to find the solution announces it to others on the network. The other miners then check whether the sender of the funds has the right to spend the money, and whether the solution to the puzzle is correct.

If enough of them grant their approval, the block is cryptographically added to the ledger and the miners move on to the next set of transactions (hence the term “blockchain”). The miner who found the solution gets 25 bitcoins as a reward, but only after another 99 blocks have been added to the ledger.”

Blockchain Glossary, Terms, and Definitions

Here’s an informative glossary on blockchain terms and definitions put together by Blockgeeks:

551% Attack

When more than half of the computing power of a cryptocurrency network is controlled by a single entity or group, this entity or group may issue conflicting transactions to harm the network, should they have the malicious intent to do so.

Address

Cryptocurrency addresses are used to send or receive transactions on the network. An address usually presents itself as a string of alphanumeric characters.

ASIC

Short form for ‘Application Specific Integrated Circuit’. Often compared to GPUs, ASICs are specially made for mining and may offer significant power savings.

Bitcoin

Bitcoin is the first decentralised, open source cryptocurrency that runs on a global peer to peer network, without the need for middlemen and a centralised issuer.

Block

Blocks are packages of data that carry permanently recorded data on the blockchain network.

Blockchain

A blockchain is a shared ledger where transactions are permanently recorded by appending blocks. The blockchain serves as a historical record of all transactions that ever occurred, from the genesis block to the latest block, hence the name blockchain.

Block Explorer

Block explorer is an online tool to view all transactions, past and current, on the blockchain. They provide useful information such as network hash rate and transaction growth.

Block Height

The number of blocks connected on the blockchain.

Block Reward

A form of incentive for the miner who successfully calculated the hash in a block during mining. Verification of transactions on the blockchain generates new coins in the process, and the miner is rewarded a portion of those.

Central Ledger

A ledger maintained by a central agency.

Confirmation

The successful act of hashing a transaction and adding it to the blockchain.

Consensus

Consensus is achieved when all participants of the network agree on the validity of the transactions, ensuring that the ledgers are exact copies of each other.

Cryptocurrency

Also known as tokens, cryptocurrencies are representations of digital assets.

Cryptographic Hash Function

Cryptographic hashes produce a fixed-size and unique hash value from variable-size transaction input. The SHA-256 computational algorithm is an example of a cryptographic hash.

Dapp

A decentralised application (Dapp) is an application that is open source, operates autonomously, has its data stored on a blockchain, incentivised in the form of cryptographic tokens and operates on a protocol that shows proof of value.

DAO

Decentralised Autonomous Organizations can be thought of as corporations that run without any human intervention and surrender all forms of control to an incorruptible set of business rules.

Distributed Ledger

Distributed ledgers are ledgers in which data is stored across a network of decentralized nodes. A distributed ledger does not have to have its own currency and may be permissioned and private.

Distributed Network

A type of network where processing power and data are spread over the nodes rather than having a centralised data centre.

Difficulty

This refers to how easily a data block of transaction information can be mined successfully.

Digital Signature

A digital code generated by public key encryption that is attached to an electronically transmitted document to verify its contents and the sender’ s identity.

Double Spending

Double spending occurs when a sum of money is spent more than once.

Ethereum

Ethereum is a blockchain-based decentralised platform for apps that run smart contracts, and is aimed at solving issues associated with censorship, fraud and third party interference.

EVM

The Ethereum Virtual Machine (EVM) is a Turing complete virtual machine that allows anyone to execute arbitrary EVM Byte Code. Every Ethereum node runs on the EVM to maintain consensus across the blockchain.

Fork

Forks create an alternate version of the blockchain, leaving two blockchains to run simultaneously on different parts of the network.

Genesis Block

The first or first few blocks of a blockchain.

Hard Fork

A type of fork that renders previously invalid transactions valid, and vice versa. This type of fork requires all nodes and users to upgrade to the latest version of the protocol software.

Hash

The act of performing a hash function on the output data. This is used for confirming coin transactions.

Hash Rate

Measurement of performance for the mining rig is expressed in hashes per second.

Hybrid PoS/PoW

A hybrid PoS/PoW allows for both Proof of Stake and Proof of Work as consensus distribution algorithms on the network. In this method, a balance between miners and voters (holders) may be achieved, creating a system of community-based governance by both insiders (holders) and outsiders (miners).

Mining

Mining is the act of validating blockchain transactions. The necessity of validation warrants an incentive for the miners, usually in the form of coins. In this cryptocurrency boom, mining can be a lucrative business when done properly. By choosing the most efficient and suitable hardware and mining target, mining can produce a stable form of passive income.

Multi-Signature

Multi-signature addresses provide an added layer of security by requiring more than one key to authorize a transaction.

Node

A copy of the ledger operated by a participant of the blockchain network.

Oracles

Oracles work as a bridge between the real world and the blockchain by providing data to the smart contracts.

Peer to Peer

Peer to Peer (P2P) refers to the decentralized interactions between two parties or more in a highly-interconnected network. Participants of a P2P network deal directly with each other through a single mediation point.

Public Address

A public address is the cryptographic hash of a public key. They act as email addresses that can be published anywhere, unlike private keys.

Private Key

A private key is a string of data that allows you to access the tokens in a specific wallet. They act as passwords that are kept hidden from anyone but the owner of the address.

Proof of Stake

A consensus distribution algorithm that rewards earnings based on the number of coins you own or hold. The more you invest in the coin, the more you gain by mining with this protocol.

Proof of Work

A consensus distribution algorithm that requires an active role in mining data blocks, often consuming resources, such as electricity. The more ‘work’ you do or the more computational power you provide, the more coins you are rewarded with.

Scrypt

Scrypt is a type of cryptographic algorithm and is used by Litecoin. Compared to SHA256, this is quicker as it does not use up as much processing time.

SHA-256

SHA-256 is a cryptographic algorithm used by cryptocurrencies such as Bitcoin. However, it uses a lot of computing power and processing time, forcing miners to form mining pools to capture gains.

Smart Contracts

Smart contracts encode business rules in a programmable language onto the blockchain and are enforced by the participants of the network.

Soft Fork

A soft fork differs from a hard fork in that only previously valid transactions are made invalid. Since old nodes recognize the new blocks as valid, a soft fork is essentially backward-compatible. This type of fork requires most miners upgrading in order to enforce, while a hard fork requires all nodes to agree on the new version.

Solidity

Solidity is Ethereum’ s programming language for developing smart contracts.

Testnet

A test blockchain used by developers to prevent expending assets on the main chain.

Transaction Block

A collection of transactions gathered into a block that can then be hashed and added to the blockchain.

Transaction Fee

All cryptocurrency transactions involve a small transaction fee. These transaction fees add up to account for the block reward that a miner receives when he successfully processes a block.

Turing Complete

Turing complete refers to the ability of a machine to perform calculations that any other programmable computer is capable of. An example of this is the Ethereum Virtual Machine (EVM).

Wallet

A file that houses private keys. It usually contains a software client which allows access to view and create transactions on a specific blockchain that the wallet is designed for.

Blockchain Slang

Last, but not least, here’ s a glossary of blockchain slang to help you as you read more about blockchain and blockchain applications:

#ALTCOIN = Any crypto currency other than bitcoin.

#ASHDRAKED = A situation where you lost all your money.

#BAGHOLDER = A person who buys and hold coins in large quantity hoping to make good profits in the future.

#BEAR/BEARISH = Negative price movement

#BTFD = Buy The Fucking Dip (an indication to buy a coin when it has dumped so hard)

#BULL/#BULLISH = Positive price movement

#DILDO = Long green or red candles

#DUMP = To Sell off a coin

#DUMPING = Downward price movement

#DYOR = Do Your Own Research

#FA = Fundamental Analysis

#FOMO = Fear Of Missing Out (A coin is pumping and you get the feeling it’s gonna pump more, so you buy high)

#FUD = Fear Uncertainty & Doubt

#HODL = Hold/Hold a position

#JOMO = Joy Of Missing Out

#LONG = Margin bull position

#MCAP = Market Capitalization

#MOON = Continuous upward movement of price

#OTC = Over The Counter

#PUMP = Upward price movement

#SAJ #CANDLE = Huge green candle

#SHITCOIN = A coin with no potential value or use

#SHORT = Margin bear position

#SWING = Zig zag price movement (Upwards and downwards)

#TA = Technical Analysis

REKT = When you have a bad loss

REVERSE INDICATOR = Someone who is always wrong predicting price movements.

RSI = Relative Strength Index

WHALE = Very Wealthy trader/Market mover