**BLOCKCHAIN**

**Definition**

A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. Harvard Business Review defines it as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, or food traceability.

**Where It All Started**

Blockchain technology was first introduced in a whitepaper entitled: “Bitcoin: A Peer-to-Peer Electronic Cash System,” by Satoshi Nakamoto in 2008.

* No reliance on trust
* Digital signatures
* Peer-to-peer network
* Proof-of-work
* Public history of transactions
* Honest, independent nodes control majority of CPU computing power
* Nodes vote with CPU computing power
* Rules and incentives enforced through consensus mechanism

**Cryptocurrency Summarized**

* Bitcoin was the first digital, i.e., cryptocurrency
* A maximum of 21 million Bitcoins can be generated
* Just as with real world mining, energy must be invested to solve complex mathematical problems by which systems earn Bitcoins
* <https://www.cryptocoincharts.info/coins/info> claims to be indexing 4,220 cryptocurrencies
* Most circulated: Bitcoin, Ethereum, Litecoin

**The Technology Behind Bitcoin**

* Think of Bitcoin as an electronic asset (as well as a digital currency)
* A network of computers keeps track of Bitcoin payments, and adds them to an ever-growing list of all the Bitcoin payments that have been made, called “The Bitcoin Blockchain”
* The file that contains data about all the Bitcoin transactions is often called a “ledger”
* Bitcoin value is created through transaction processing, referred to as “mining,” which is performed by distributed processors called “nodes” of the peer-to-peer network

**Mining Evolution**

* Mining is the process whereby value is created through transaction processing that occurs on nodes of the network.
* In 2009, one could mine 200 Bitcoins with a personal, home computer. In 2015, it would take about 98 years to mine just 1 Bitcoin.
* Today there is almost no money to be made through traditional home mining.
* ASIC (Application Specific Integrated Circuit) has been designed strictly for mining Bitcoins.
* Groups of miners have formed mining pools, with each being paid their relative share for their contribution to the work performed.

**Three “Levels” of Blockchain**

1. Storage for digital records
2. Exchanging digital assets (called tokens)
3. Executing smart contracts
   * Ground rules – Terms & conditions recorded in code
   * Distributed network executes contract & monitors compliance
   * Outcomes are automatically validated without third-party

**A General Discussion about Tokens**

* A broader use is supported by the digital infrastructure introduced through Bitcoin, as represented by “tokens”.
* A “token” can be defined as a “scarce digital asset based on underlying technology inspired by Bitcoin.”
* Tokens may use similar codebases but different blockchain databases.
* Ethereum was Bitcoin-inspired but has its own blockchain and is engineered to be more programmable. Tokens can be issued on top of the Ethereum blockchain.
* Token buyers are buying private keys, which are similar to API keys, but can be transferred to other parties without consent.
* Tokens have a value and therefore a price.
* Tokens are a new model for technology and can be an alternative to equity-based financing.
* Tokens do not dilute capital. They introduce a huge increase to buyer base and time-to-liquidity.
* Token launches differ from equity sales; however, they can be issued as a way to share profits.
* Tokens can be sold internationally over the internet and are always open for business.
* Tokens decentralize the process of funding technology.
* Tokens enable a better-than-free new business model.
* Tokens will introduce the rise of the “tech savvy senior executive.”
* Tokens accommodate immediate custody without an intermediary.
* Tokens can be extended to hardware, as part of the internet of things.

**Smart Contracts**

Current paper-based systems drive $18 trillion in transactions per year. Consensus protocols are key to determining the sequence of actions resulting from the contract’s code. This enables peer-to-peer trading of everything from renewable energy to automated hotel room bookings.