A History of Blockchain

Pre-2014: Much of blockchain's development and media attention was actually related to Bitcoin.

The price of Bitcoin in USD over time

10/31/2008 ⇒ Satoshi Nakamoto publishes a white paper that introduces the world to Bitcoin.
01/03/2009 ⇒ The first collection of transactions (called the Genesis Block) was created.
05/22/2010 ⇒ For 10,000 BTC ($25 at the time), the first Bitcoin purchase occurred. The item purchased was a pizza.
02/09/2011 ⇒ Bitcoin achieves parity with the USD ($1 USD = 1 BTC).

Post-2014: Bitcoin's value rises, and speculation on how blockchain, the technology behind Bitcoin, can be applied elsewhere emerges.

January 2014 ⇒ Blockchain technology startups (like Gem and R3) emerge.
April 2015 ⇒ NASDAQ commits to a blockchain trial, signalling enterprise level validation for the use of blockchain within finance.
10/03/2016 ⇒ Distributed:Health, the first ever blockchain centric healthcare conference occurs.
December 2017 ⇒ Bitcoin crashes totally.

Anthony Castillo
Spring 2018

Writing 105SW
393080-7

Sources:

1) https://medium.com/crypto-currently/lets-build-the-tiniest-blockchain-e70965a248b

2) https://gist.github.com/aunyks/8f2c2fd51cc17f342737917e1c2582e2

3) https://searchcompliance.techtarget.com/definition/smart-contract

4) https://www.investopedia.com/terms/c/cryptocurrency.asp

5) Computer Science 8; Prof. Omer Egecioglu; Fall 2016; UCSB

6) https://blog.gem.co/the-blockchain-timeline-3fdffe281378

7) https://www.i-scoop.eu/blockchain-distributed-ledger-technology/blockchain-iot/

8) https://hackernoon.com/bitcoin-ethereum-blockchain-tokens-icos-why-should-anyone-care-890b868cec06

9) https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo

10) https://news.bitcoin.com/the-bitcoin-bch-block-explorer-explodes-with-blockchain-data/

Blockchain 101

An intuitive introduction to the greatest decentralized computational technology created within the 21st century.

By
Anthony Castillo
2nd Year Actuarial Science Major
University of California, Santa Barbara

What is Blockchain?

Blockchain is a digital ledger system in which new data are stored in a block and then are added to an immutable chain that contains previously existing data (hence blockchain). All transactions to the ledger system are recorded chronologically and publicly, and therefore cannot be deleted from the database.

The Bitcoin logo, a popular blockchain development and cryptocurrency.

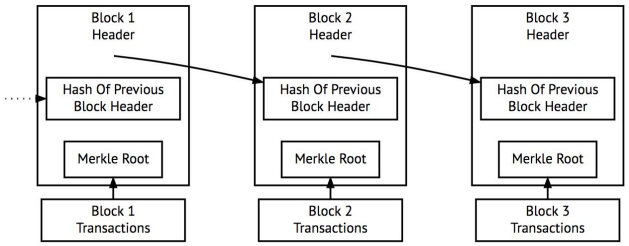
Why Blockchain?

Blockchain technologies are expected to greatly impact how society operates in the coming years. From health records to financial technology, many experts agree blockchain is expected to integrate itself into our everyday life the same way the Internet has. Based on the latest technologies and developments, I predict that in three decades, this sweeping paradigm shift will occur in almost every major industry.

How Blockchain Works

Since blockchain is entirely decentralized and distributed, all transactions occur on a peer-to-peer network where all who have access to this network can see the immutable list of transactions that are recorded on the blockchain. Each block in a blockchain contains:

1) A record of recent transactions
2) A reference to the previous block (such as a hash of a previous block header)
3) An answer to a difficult math problem (such as a Merkle Root)



Simplified Bitcoin Block Chain

Important Definitions:

Block ⇒ a singular unit of a blockchain which contains large amounts of transactional data

Hash ⇒ the unique digital signature of a block

Header ⇒ the block component that contains its metadata (such as a hash of a previous block, a Merkle Root, or a list of recent transactions)

Merkle Root ⇒ the root of a Merkle tree; the root summarizes the transactions in that block

Transaction ⇒ an appendage to the ledger system (which can be thought of as a Bitcoin transaction recorded onto the blockchain).

Applications

Cryptocurrency:

A digital currency independent of any central government or bank. Transactions are pseudonymous and public, and cryptocurrency tokens are normally generated from some type of algorithm or encryption technique. Popular examples of cryptocurrencies include bitcoin, litecoin, and ethereum.

Smart Contracts:

Self-executing contracts whose terms of agreement are in fact written in code. The code (and by extension, the agreement between all parties involved) exist across a distributed, decentralized blockchain network. Also known as a crypto contract. The contract automatically knows when to enforce obligations and issue penalties between parties.

Internet of Things:

The interconnection (via the Internet) of the everyday devices we use. This connection allows these devices to send and receive data amongst themselves since IoT applications are already distributed (meaning consensually shared and synchronized across multiple institutions). Blockchain developments and technologies would be used to speedily transact the data between these devices while securing the data along with the transaction itself.