An Overview of
Blockchain, Bitcoin and CryptoEconomics

John P. Conley
Vanderbilt University

San Francisco/Bay Area Vanderbilt Alumni Chapter

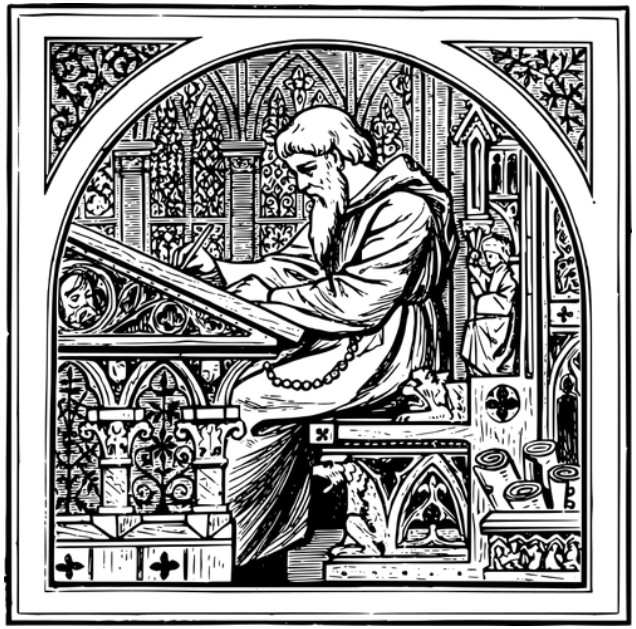
November 13, 2018

What is Blockchain?

Paper ledger books keep records of account balances, ownership of property, marriages, births, deaths etc.

Checks or charges made by the account owner were used to **update the balance** held in the account.

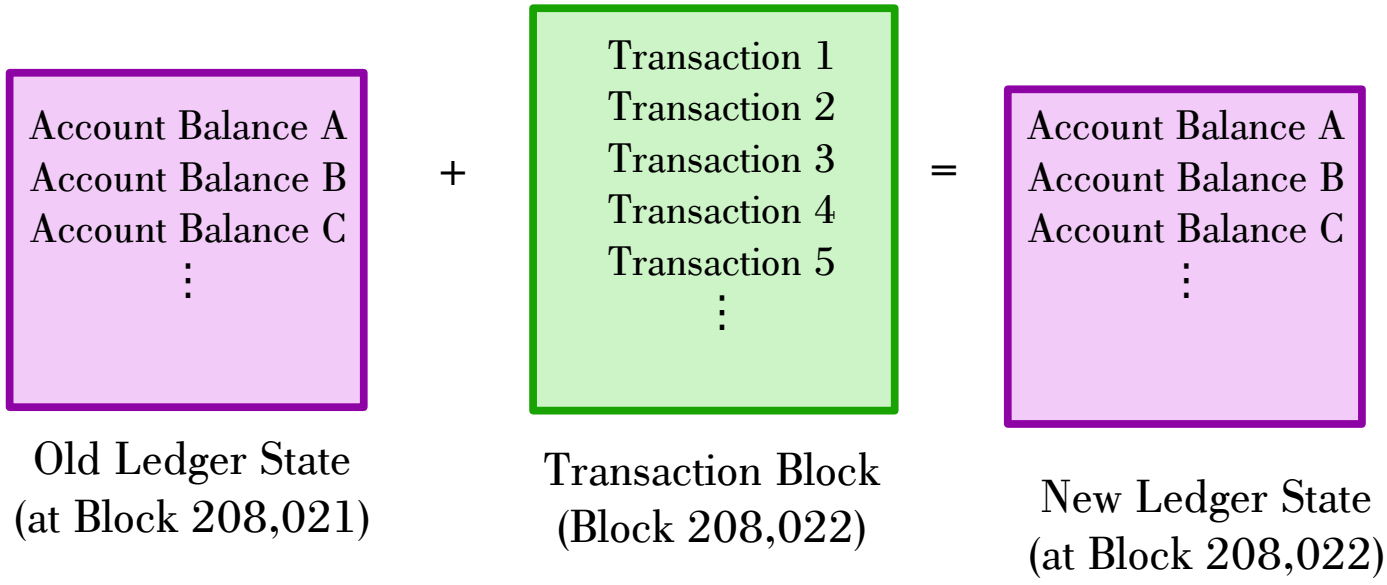
A sale of property would also result in a ledger update.



A New Way of Doing the Same Thing

Blockchain is just a ledger that groups transactions together in a sequence of “blocks” and then uses them to update the ledger state.

Blockchains are **transition-state machines**.



How Does a Blockchain Work?

1. Users submit transactions requests to **anonymous nodes** on a **peer-to-peer network.** (Also called **gossip networks**.)

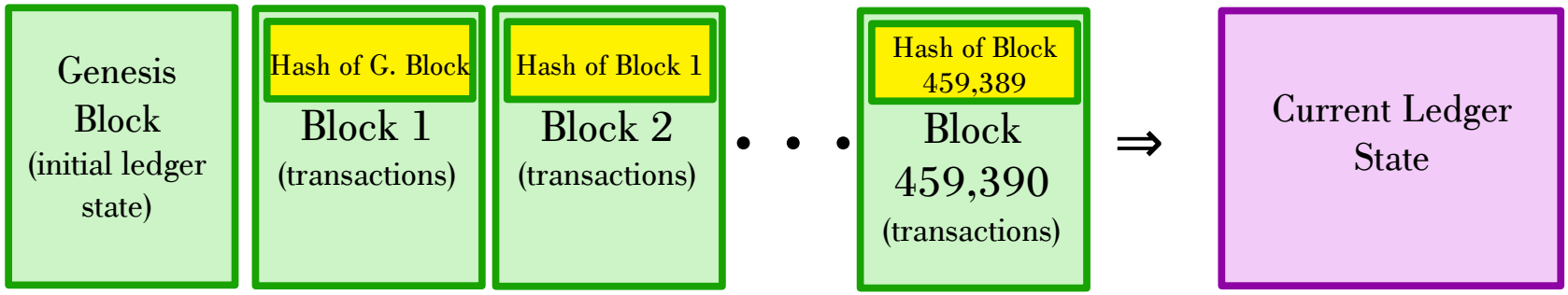
2. Nodes forward the transaction requests they receive to all other nodes.

3. Each node collects a group of transactions (about a 1000 to 2000 in the case of Bitcoin) in a **block**.

4. Each node checks the current ledger state to see if these transactions are **valid.**
   - Enough in the account to cover the transaction?
   - No double spending?
   - No forged signatures on the transactions?

5. The block of valid transactions is **appended** to the existing chain, the ledger state is updated, and then nodes start to work on a new block.

The Blockchain



Look! A squirrel!

(Add hand-waving here)

Proof of Work
Proof of Stake
Proof of Honesty
Governance
Directed Acyclic Graphs
Lightning Networks
Merkle Trees

Public-Private Encryption Keys
Mining
Smart Contracts
ERC20 Tokens
Security Tokens
Utility Tokens
Permissioned Ledgers

What's New Here?

1. **Distributed**: Thousands of nodes in the validation network keeping copies of the blockchain and ledger state.

2. **Immutable**: Cryptographic magic makes it impossible (or at least difficult) to change any transaction in a block or rewrite history.

    - Hashing of the contents of each block
    - Recursive **hashing** of blocks to link them together sequentially
    - Proof of Work (PoW) to make it computationally impractical to rewrite history

3. **Append Only**: Blocks can only be added to the end of the chain sequentially.

What Else is New Here?

4. **Uncensorable**: There is no "Bitcoin Inc." or other entity that is in charge of blockchains. Blockchains live in the wild without a central point of control. (Although this is not true for certain private permissioned blockchains.)

5. **Anonymity**: Owners of accounts are anonymous, Accounts are identified only by numbers called **public keys**. Validating nodes are sometimes anonymous as well.

6. **Cryptocurrencies and Tokens**: Blockchains can support currencies and tokens that can be used for a variety of purposes.

Important to Understand These Relationships

Blockchain ≠ Bitcoin

Cryptocurrency ≠ Cryptotokens

Blockchain ⇏ Cryptotokens

Data System ⊂ State Machine Replication System ⊂

Distributed Ledger Technology ⊂ Blockchain

Can I has Blockchain?

Sure!

The question is: Does You Want Blockchain?

Why Blockchain?

A basic question is: Why use blockchain instead of an ordinary database?

Since blockchains are ledgers, they don't have tables, metadata, or relational structures that allow for complicated SQL queries. However:

- Creates provable audit trails
- Consensus on the order of transactions
- Can't be censored
- Can't be altered
- No need for a **trusted authority** or **data intermediary**
- Facilitates **distributed business processes**
- Can support a cryptocurrency or other **cryptotoken.**

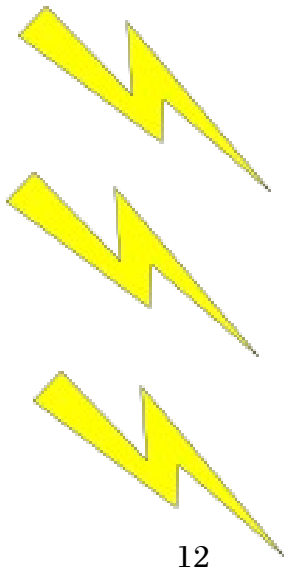
Why a Cryptocurrency?

Let's begin by remembering the basic economics of money.

First, what is it good for? Absolutely nothing. Say it again!

Fiat currencies, such as US federal reserve notes, have no intrinsic value.

They are simply pieces of paper that have been enchanted by the Treasury Wizards.



Why a Cryptocurrency?

Cryptocurrencies are the same. They have utility primarily as **mediums of exchange** and **stores of value.**

There is no reason bitcoin could not be used instead of dollars. It just takes mass agreement.

Dollars, however, cannot take the place of cryptocurrencies.

Blockchain can only control data and tokens that are native to the chain.

Blockchains cannot immutably move dollars from account to account because dollars are controlled by banks and governments and don't live on the chain.

Why a Cryptocurrency?

Therefore:

The main purpose of a cryptocurrency is allow the users of a blockchain to **pay for validation, virtual machine, and other service**s on a given platform.

This allows users to **compensate and incentivize validators** to maintain the blockchain honestly.

Cryptocurrencies can also be used for **micropayments** and as low transactions cost scrip within a blockchain ecosystem.

There are no other significant reasons that a blockchain platform should have a native cryptocurrency.

Why a Token?

Cryptotokens have many potential uses besides being a form of money.

Tokens can represent stocks, bonds, land or car titles. (**Tokenization** of real and financial assets)

If these are legally recognized, then we could represent each share of Microsoft, for example, with a token and then keep a ledger that shows and updates how they are distributed and owned.

This can facilitate low cost, high security, stock exchanges.

Blockchain based exchanges could preserve the owners' **anonymity** or be part of crypto-exchange systems on **smart contracts** that automatically kept **audit trials** for compliance and tax reasons.

Stocks are homogeneous goods, so you only need to know how many shares you own.

Why a Token?

Land, car, and other **property titles** are individual items that could be represented with **uniquely identified tokens** and then traded in a similar way.

Ownership could also be **fractionalized** and turned into **derivatives**, at assuming the existence of a supporting legal structure.

Tokens could be used to represent **voting power** or certain types of **access or privilege** on a platform, or entitle the owners to **shares** of certain revenue streams. (These are sometimes called **Security Tokens.**)

Use Cases

Payment networks:

- Micropayments
- Smart cities
- Escrows
- Internal payment networks (Commodore Card)

Tokenized markets:

- Stocks
- Derivatives
- Property and loans
- Venture capital and startups

Internet of things (IoT)

- Two-sided markets between devices
- Economic interaction with real world agents
- Accountability
- Liability

Distributed business processes

Logistics
Provenance
Accountability (Opioids, maintenance, inventory)
Real estate transactions
Medical records

Public Records:

property titles
Legal records
Identity
Education and certification
Transparency (potholes)

.

Are Cryptocurrencies a Ponzi Scheme?

Bitcoin, Ethereum, and all other cryptocurrencies have no intrinsic value.

They are only worth what the next person will pay for them.

Sounds like a Ponzi scheme that depends on the existence of the greater fool, right?

Blockchain is Really Dot Com 2.0

First:

- Bitcoin and blockchain are **not the same**.
- Not all cryptotokens are cryptocurrencies.
- Not all blockchains need a cryptotoken to provide utility.

Second:

- Most blockchain startups are about as well conceived as pets.-com.
- Most blockchain startups do not really need a token but have one anyway to raise money.
- Many blockchain startups do not really need blockchain. It's just cooler that way.

Third:

- For every 99 pets.com or webvan.com, there was a google.com as well.

In Other Words

Blockchain is like the Internet in 1998. We just don't have a clear idea yet of where it will provide the greatest value or how.

(Actually, more like the Internet in 2002, the bottom of the hype cycle)

Blockchain is going to bring on a wave of disintermediation and creative disruption in a vast array of industries.

Wrapping Up

Blockchain is relatively new and over-hyped.

Blockchain startups are mostly badly conceived.

Enterprises, governments, NGOs and others think they want blockchain, they just don't know how or why.

Blockchain is often a solution looking for a problem.

Getting rich speculating on cryptocurrencies is a matter of luck and timing. If you have them, blessings on your house. This ship has probably sailed

Nevertheless, blockchain is coming, it is going to be big, and it is going to provide enormous value in a wide array of verticals.

Thanks For Listening!

If this has not left you completely fed-up with blockchain have a look at:

www.jpconley.com

for other things I have written on initial coin offerings, a simple explanation of hashing, encryption, and blockchain, permissioning on public blockchains, tokenizing dollars, cloud computing, and other related topics.