

An Introduction to Blockchain, Bitcoin, and CryptoEconomics

John P. Conley
Vanderbilt University

Tennessee Tech University

Window on the World

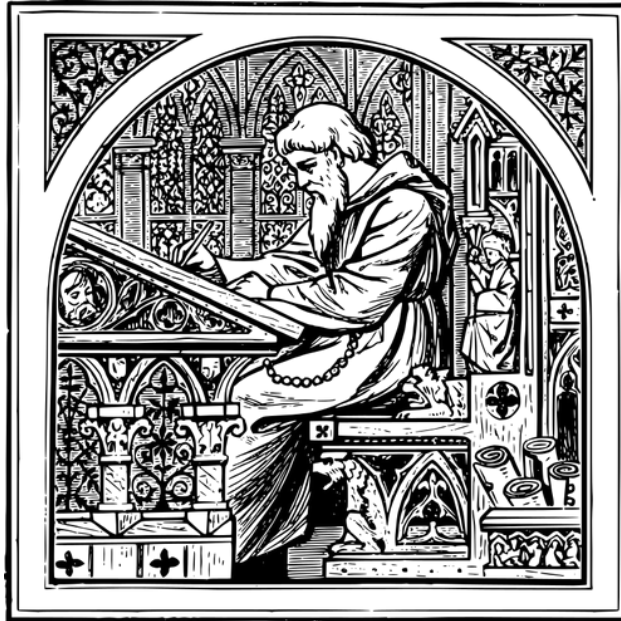
April 2018

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.

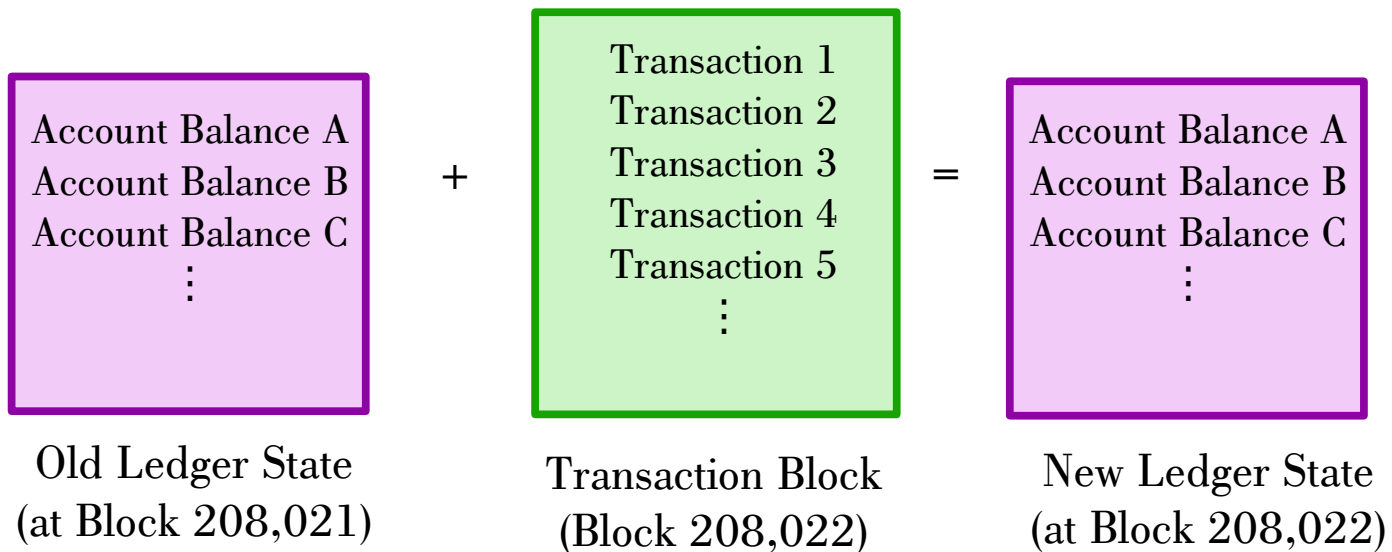
A sale of property would also result in a ledger update.



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.

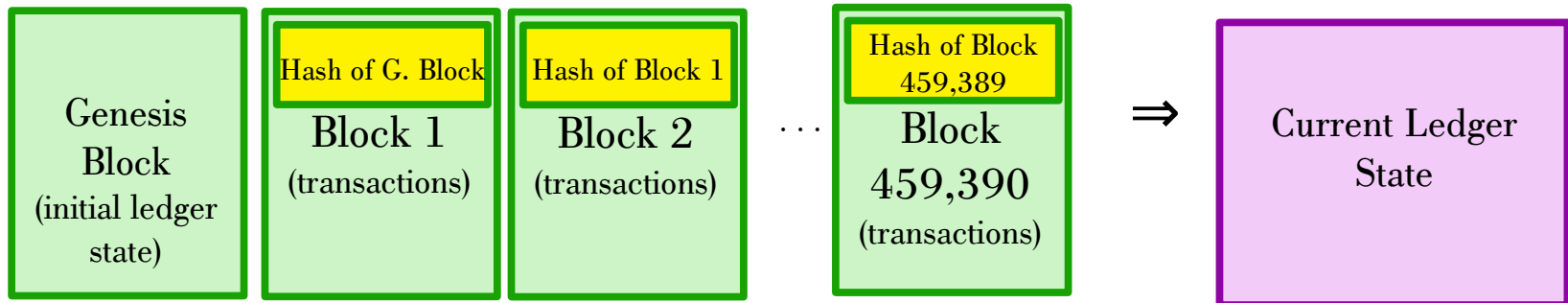
Blockchains are **transition-state machines**.



How Does Blockchain Work?

1. Users submit transactions requests to **anonymous nodes** on a **peer-to-peer network**.
2. Nodes forward the transaction requests they receive to all other nodes (peer-to-peer networks are sometimes called **gossip networks**.)
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
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. **Time-Stamps:** Time stamps in the blockchain prove when a transaction was written.
5. **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.)
6. **Anonymity:** Owners of accounts are anonymous, Accounts are identified only by numbers called **public keys**. Validating nodes are sometimes anonymous as well.

Why a 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.

Validation through **Proof of Work** is expensive, complex, and sometimes not very secure.

Bitcoin writes a 1MB block every ten minutes. Ethereum has similar limits.

Proof of Stake and Directed Acyclic Graph (DAG) solutions make other types of compromises.

BUT

- ◆ Creates provable audit trails
- ◆ Time stamps
- ◆ Can't be censored
- ◆ Can't be altered
- ◆ No need for a **trusted authority** or **data intermediary**
- ◆ Facilitates **distributed business processes**
- ◆ Can support a crypto-token

Tokens?

A token is just an **accounting entry** in the blockchain ledger as in: “Fred owns 57 TechTokens”. They have no other existence, and cannot move from the chain where they were created.

Bitcoin, Ethereum are the two most well known crypto-tokens. All Bitcoins are recorded in the Bitcoin blockchain and nowhere else.

However, there are many more. From <https://coinmarketcap.com/>:













Cryptocurrencies: **1565** / Markets: **10245** Market Cap: **\$312,083,451,609** / 24h Vol: **\$24,995,911,039** / BTC Dominance: **42.9%**

Cryptocurrencies are a special case of crypto-tokens with no other use than a unit of exchange (like dollars).

Crypto-tokens, more generally, can do many other things.




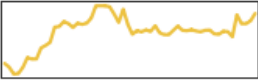






Token Caps

Also from <https://coinmarketcap.com/>

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$133,746,769,231	\$7,879.45	\$8,935,520,000	16,974,125 BTC	13.50%	
2	 Ethereum	\$48,402,633,982	\$489.99	\$2,540,980,000	98,782,902 ETH	13.95%	
3	 Ripple	\$23,877,111,243	\$0.610312	\$1,317,350,000	39,122,794,968 XRP *	15.42%	
4	 Bitcoin Cash	\$12,579,765,224	\$736.96	\$418,246,000	17,069,900 BCH	10.76%	
5	 Litecoin	\$7,112,634,411	\$126.89	\$581,244,000	56,055,313 LTC	8.49%	
6	 EOS	\$6,732,132,319	\$8.53	\$1,650,040,000	788,779,714 EOS *	1.33%	

As of Thursday April 12, 2018

So Much Token Cap!

111	 Achain	\$102,353,214	\$0.218035	\$21,284,800	469,434,790 ACT *	19.20%	
112	 High Performa...	\$100,763,803	\$3.39	\$6,664,490	29,702,632 HPB *	9.57%	
113	 Nexus	\$100,307,721	\$1.77	\$2,242,430	56,682,878 NXS	3.85%	
114	 Genaro Network	\$96,109,548	\$0.402556	\$5,666,600	238,748,268 GNX	7.62%	
115	 Vertcoin	\$95,633,117	\$2.19	\$2,757,810	43,754,400 VTC	7.04%	

113 Blockchain platforms have token caps above \$100M.

Not an Equity!

How do we interpret this token cap?

How should we think about valuing crypto-tokens?

If tokens were like stocks, then they should be worth the **Present Value (PV)** of the associated flow of dividends:

$$\sum_{t=0}^T (1-r)^t \pi_t$$

Tokens, however, are not like stocks.

When you buy a token you are not buying a share of the company that issued it.

In almost every case you are not even buying the right to share in the company's profits or vote on its board of directors.

By this measure, the value of most crypto-tokens should be very close to zero.

Speculation?

Bitcoin has increased in value from \$1200 to \$8,000 over the last year, and reached a high of almost \$20,000 in December of 2017.

You should buy it now before it goes up more, right?

Efficient Market Theory (EMT) says that the best predictor of tomorrow's price is today's price.

Put another way, today's price is tomorrow's expected price:

$$p_t = E(p_{t+1})$$

Otherwise, there would be an **arbitrage opportunity**.

This means that prices are heavily dependent on **expectations** and the **arrival of new information**.

By this measure, the value of most crypto-tokens could be anything. All that is needed is the right set of expectations.

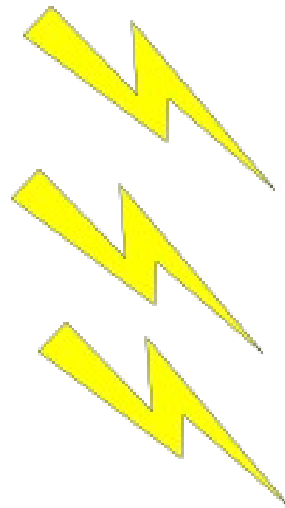
Monetary Theory?

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*.



Do you Believe in Magic?

Why are we willing to take these paper tokens in exchange for things of real value?

Because we trust that others will take the same pieces of paper in exchange for things of value in the future.

This leads to one of the fundamental rules of monetary theory:

Money is Trust

At a more practical level, money serves three distinct purposes:

Medium of Exchange: Solves the **mutual coincidence of wants** problem.

Store of Value: If a currency is relatively stable, it can be saved to buy goods in the future.

Unit of Account: Allows us to keep track of the value of things relative to one another.

Quantity Theory of Money

M = Money supply (number of tokens).

P = Price of tokens in terms of dollars.

T = Total number of tokens transacted per day.

V = Velocity of Token (number of times a bitcoin is transacted per day).

D = Dollar Value of total transactions per day (PT=D).

The QTM is an accounting identity that says the following:

$$T=MV$$

For example, if there are 100 tokens that each trade 2 times a day then 200 tokens will be traded each day.

More interestingly

$$D/P = MV \text{ or } P = D/MV$$

For example:

Suppose that I issue 100 goat tokens ($M=100$)

Each token trades twice a day ($V=2$)

800 goats are bought and sold each day using my tokens ($D=800$).

Then each token must be worth 4 goats ($P=4$) since there are 200 token transactions per day ($T=200=100 \times 2$).

Really? That's More Interesting?

As of Thursday April 12, 2018:

\$8k = P = Price of a bitcoin

17M = M = Total number of bitcoins

\$134B = PM = Bitcoin market cap

\$9B = PT = Value of bitcoin transactions per day

1.1M = T = $9B/8k$ = Number of bitcoins traded per day.

.066 = V = $T/M = PT/PM = 1.1M/17M$ = Velocity of bitcoins

In words, about 6.6% of bitcoins move each day.

As a result, in order to support \$9B worth of transactions per day using only 17M bitcoins having a velocity of .066, bitcoins must have a value of \$8,000 each.

Still Not Seeing It?

What drives the value of bitcoin (or any token) is:

1. The demand to support a certain value of transactions per day.
2. The velocity of tokens.
3. The number of tokens.

Transaction Demand is decided by users. The level and value of economic activity in a country or on a platform comes from choices of agents in the economy. The more users, the greater the value of things traded on the platform, and the more often things are traded, the greater D will be and so, therefore, will be the value of token, P .

Velocity is also determined by user choices. However, platforms can be designed to slow down velocity. For example, if tokens are used for stakes, are put into escrow, need to be locked up or held to do something on the platform, or if transactions are slow to complete, velocity is lower and token value higher.

Token Quantity is chosen by the platform. If a platform is going to issue a lot of tokens, then token value goes down, all else equal.

Why is Bitcoin so Volatile?

Bitcoin has gone up in value about 700% over the last year.

In 2018 bitcoin as fluctuated between \$6k and \$15k and in 2017 Between \$0.8k and \$20k.

Let's go back the QTM.

Suppose we wanted to support \$9B in transactions value per day, as before.

Bitcoin blocks are written every 10 minutes, so $6 \times 24 = 144$ blocks are written per day.

If each bitcoin was transacted in each block (that is, $V=144$) then 2.5B transactions could take place per day ($T=2.5B$).

As a result, \$9B of transactions could be supported with a bitcoin price of $9B/2.5B = P = \$3.60$.

What Does This Mean?

Suppose users wished to transact \$9B per day in bitcoin.

\$8,000 is an equilibrium price of bitcoin under the QTM if Velocity is .066.

\$3.60 is an equilibrium price of bitcoin under the QTM if Velocity is 144 (the maximum possible).

By the way, Ethereum writes blocks every 10 seconds, so it has a maximum velocity of $6 \times 60 \times 24 = 8640$.

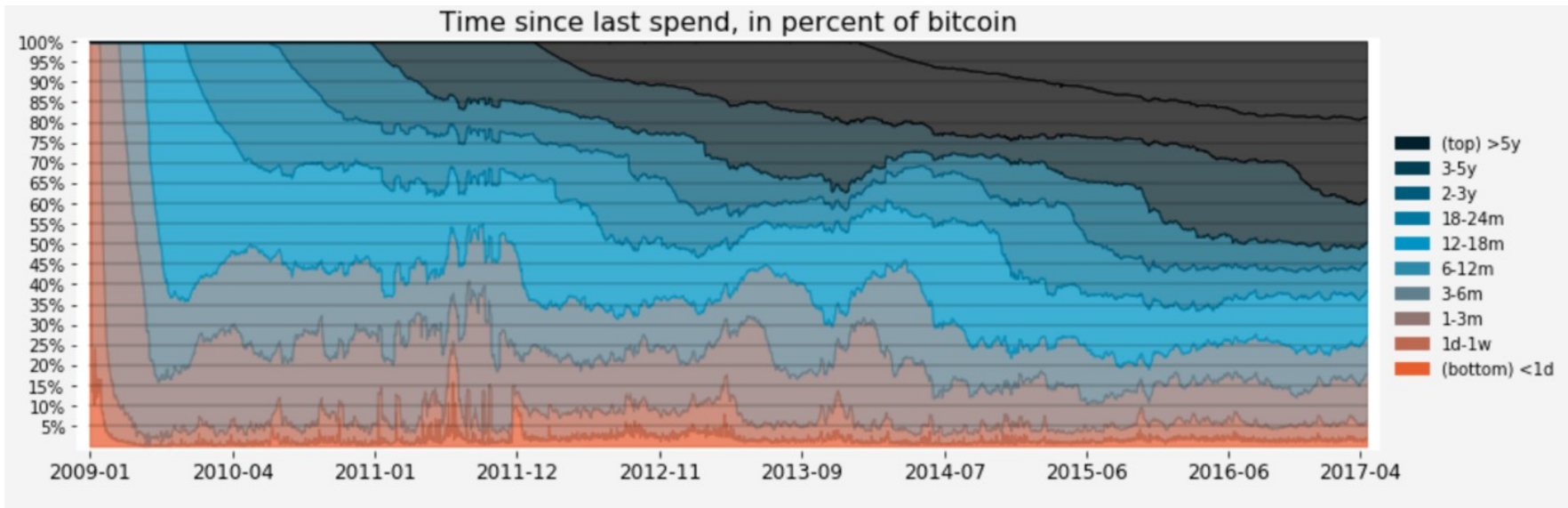
So, which is it? \$8K or \$3.60? Both are equilibria!

In fact any price above \$3.60 could be an equilibrium supporting \$9B in transactions per day depending on velocity.

In other words, there are an **infinity of possible equilibrium prices** for Bitcoin, Ethereum, and every other crypto-token that are consistent with the QTM and EMT.

In the end it depends on **animal spirits**.

Look, A Picture!



This shows at least two interesting things.

First, until quite recently, only about 2% of bitcoins moved once a day. On the average, bitcoins moved once every 80 days or so.

Second, 20% have not moved in five years, and about 50% have not moved in the two years.

In other words, most bitcoins just sit in wallets and are not used for transactions. Why is an interesting question.

Awesome!

Having said all that, Blockchain is awesome!

The NYSE will be on blockchain within five years, probably much sooner.

In addition:

- ◆ Public records will be on blockchain,
- ◆ Payment systems like Visa/MC will have moved to blockchain or been **disintermediated**.
- ◆ Connected devices (the **Internet of Things**) will use blockchain to act as agents for the owners.
- ◆ Logistics chains and other distributed business processes like real estate will use blockchain.
- ◆ Two-sided markets and matching problems such as staffing will use blockchain.
- ◆ Squirrels will be on blockchain....

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 crypto-tokens are cryptocurrencies.
- ◆ Not all blockchains need a crypto-token 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.

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

Wrapping Up

Blockchain is 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.

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

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.