

An Introduction to Blockchain, Bitcoin, and CryptoEconomics

John P. Conley
Vanderbilt University

Vanderbilt Alumni Metro New York Chapter

January 2018

What is Blockchain?

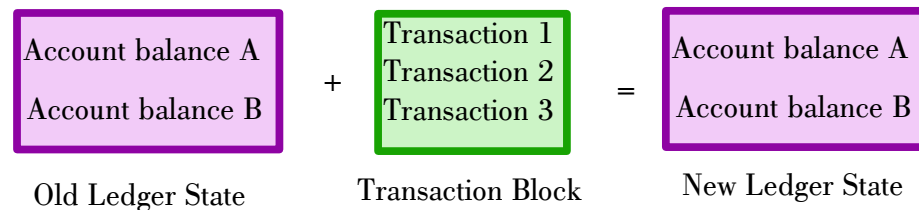
Paper ledger books keep records of account balances, ownership of property, marriages, births, deaths etc.

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.

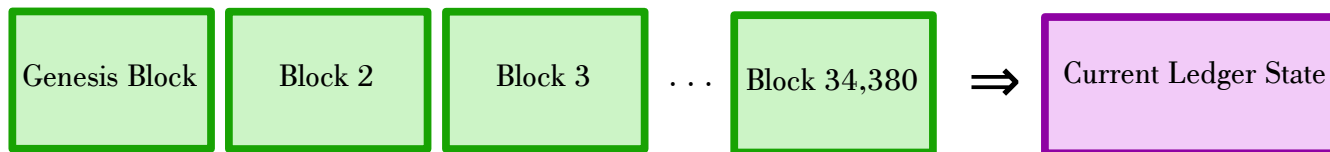
Blockchain is just a ledger that groups together transactions in “blocks” and uses them to update the ledger state.

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 to all other nodes (peer-to-peer networks are sometimes called **gossip networks**.)
3. Each node collects a group of transactions (about a 1000 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
Mining
Proof of Stake
Distributed Hash Tables
Smart Contracts
Utility Tokens
Byzantine Fault Tolerance

What's New Here?

1. **Distributed:** Thousands of nodes in the validation network. Each keeps a copy of the blockchain and ledger state.
2. **Immutable:** cryptographic magic makes it impossible to change any transaction in a block or to 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.
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. They live in the wild without a central point of control.
6. **Anonymity:** Owners of accounts are anonymous since accounts are identified only with numbers called **public keys**.

Look! Another squirrel!

Public Private Key (PPK) Encryption
Hashing Functions
Merkle Trees
Cryptographic Signatures
Permissioned Ledgers
Pseudo-Anonymity

Why a Blockchain?

A basic question is: why use blockchain instead of a standard database?

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

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

There are limits to how much data can be added to blockchains: Bitcoin writes 1MB every ten minutes.

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 Vandycoins”. 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: **1456** / Markets: **7525**




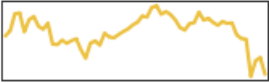








Market Cap: **\$529,033,789,631** / 24h Vol: **\$57,842,352,566** / BTC Dominance: **35.7%**

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	\$199,608,318,115	\$11,877.40	\$14,594,800,000	16,805,725 BTC	-14.36%	
2	 Ethereum	\$101,277,903,133	\$1,043.95	\$5,626,670,000	97,014,132 ETH	-21.15%	
3	 Ripple	\$51,122,884,593	\$1.32	\$3,487,100,000	38,739,142,811 XRP *	-27.62%	
4	 Bitcoin Cash	\$32,450,345,789	\$1,918.48	\$1,657,830,000	16,914,613 BCH	-21.28%	
5	 Cardano	\$16,046,834,352	\$0.618922	\$1,131,760,000	25,927,070,538 ADA *	-25.60%	
6	 Litecoin	\$10,679,755,797	\$194.96	\$870,465,000	54,780,058 LTC	-18.02%	

Tuesday January 16, 2018 was not a good day for blockchain!

Still, top six **token caps** are above \$10B

So Much Token Cap!

166	 Cindicator	\$106,407,248	\$0.073589	\$9,274,270	1,445,976,590 CND *	-22.39%	
167	 Triggers	\$105,746,462	\$3.29	\$45,448,200	32,105,578 TRIG *	-27.12%	
168	 LBRY Credits	\$105,448,752	\$0.739674	\$5,467,830	142,561,117 LBC	-31.70%	
169	 district0x	\$100,342,800	\$0.167238	\$7,682,580	600,000,000 DNT *	-25.64%	
170	 Viacoin	\$99,777,865	\$4.35	\$1,724,320	22,961,722 VIA	-28.96%	

169 Blockchain startups 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 \$900 to \$13,000 over the last year, and reached a high of \$20,000.

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 blessed by the *Treasury Wizards*.

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

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 Bitcoin (number of time 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, if we need to use 100 goat tokens to buy and sell 800 goats each day and tokens have a velocity of 2, then each token must be worth 4 goats.

Really? That's More Interesting?

Here's why.

As of Monday January 15 2018:

\$230B = PM = Bitcoin market cap

\$13B = PT = Value of bitcoin transactions per day

1M = T = 13B/13k = Number of bitcoins traded per day.

.058 = V = T/M = PT/PM = 1.M/17M = Velocity of bitcoins

In words, about 6% of bitcoins move each day.

As a result, in order to support \$13B worth of transactions per day using only 17M bitcoins having a velocity of .058, bitcoins must have a value of \$13,000 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.

These are things that you can either observe or try to estimate when deciding if a token is a good investment.

Why is Bitcoin so Volatile?

Bitcoin has gone up in value more than 10,000% over the last year.

It lost 14% of its value in one day this Monday, and has had radical swings in value both up and down over its history.

Let's go back the QTM.

Suppose we wanted to support \$13B 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, \$13B of transactions could be supported with a bitcoin price of $13B/2.5B = \$5.20$ ($P = \$5.20$).

What Does This Mean?

Suppose users wished to transact \$13B per day in bitcoin.

\$13,000 is an equilibrium price of bitcoin under the QTM if Velocity is .06.

\$5.20 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 $6 \times 60 \times 24 = 8640$.

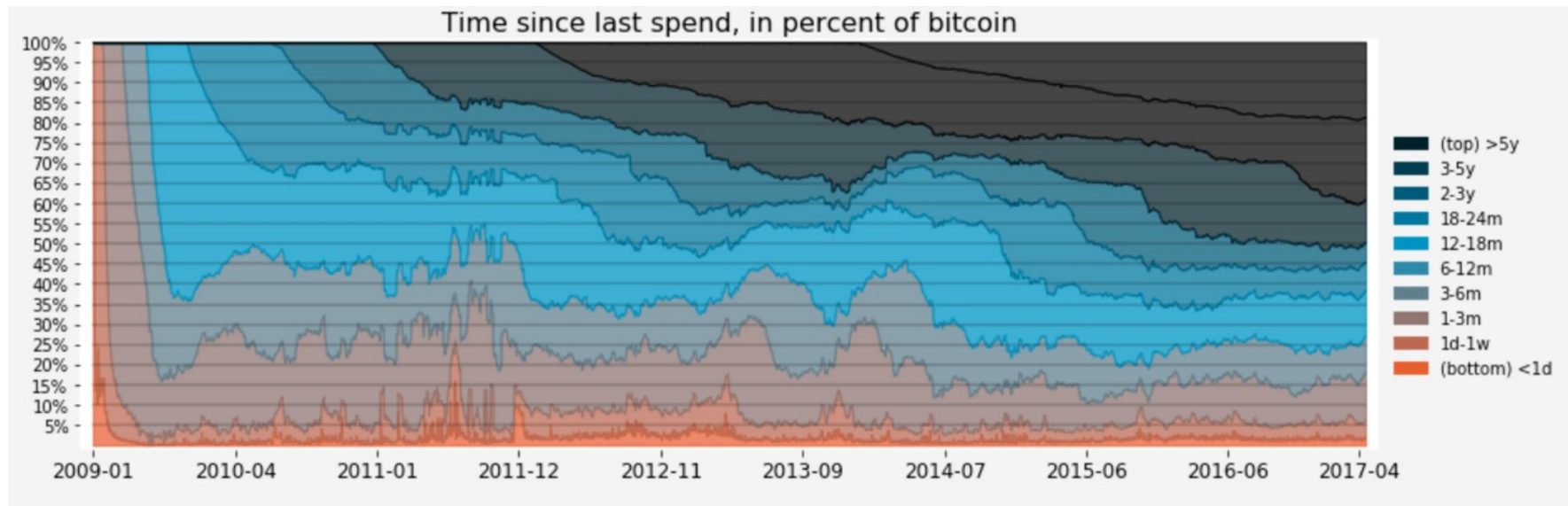
So, which is it? \$13K or \$5? Both are equilibria!

In fact any price above \$5.20 could be an equilibrium supporting \$13B 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 half 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.

Is Blockchain 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.

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

Blockchain is .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. Its just cooler that way.

Third:

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

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.

Problems

Blockchain is an immature technology. It suffers from the following major problems right now:

Cost: It costs about \$1 to make an Ethereum transaction and \$25 to make a bitcoin transaction. This is too high for either to be a practical substitute for good old fiat currency.

Scalability: Bitcoin can execute as many as 7 transactions per second, and Ethereum can do as many as 15. The Visa/MC network can execute 56,000.

Security: The security models of existing crypto-tokens is weak. Proof of Work is expensive, Proof of Stake is manipulable.

For example, it would not be wise or practical to move the NYSE onto any existing blockchain platform.

Blockchain is 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....

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.

Businesses 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 huge value.

If you want to invest, follow the same rules as always:

What is the value proposition?

What is the revenue model?

Who is the team?

Can they execute?

Do they have a comparative advantage?

Thanks For Listening



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

www.jpconley.com

for other background reading on initial coin offering, a simple explanation of hashing, encryption and blockchain, permissioning on public blockchains, tokenizing dollar, cloud computing, and other related topics.