An Introduction to
Blockchain, Bitcoin, and CryptoEconomics

John P. Conley
Vanderbilt University

Golden Triangle Angel Network

Waterloo Region, Ontario, Canada

February 2018

Agilely Pivot to New Community Directed Messaging to Leverage Core Competencies

Blockchain:
Really?

John P. Conley
Vanderbilt University

Golden Triangle Angel Network

Waterloo Region, Ontario, Canada

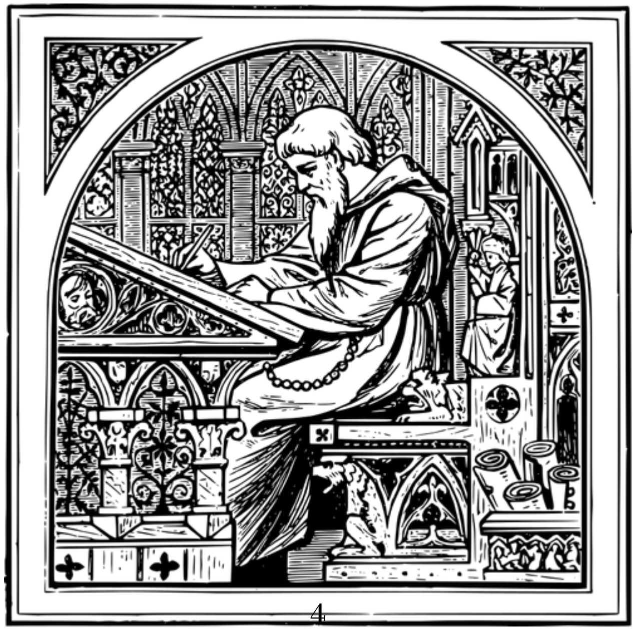
February 2018

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.

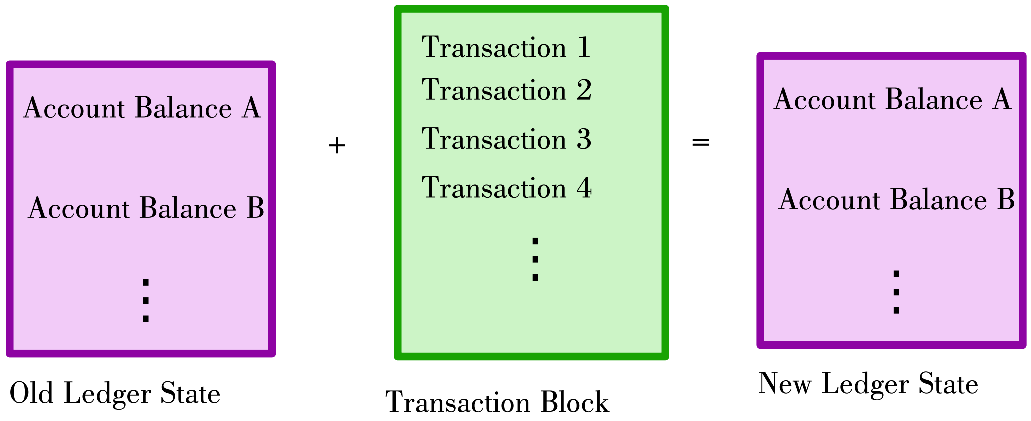
A sale of property would also result in a ledger update.



A New Way of Doing the Same Thing

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

Blockchains are **transition-state machines**.



Account Balance A

Account Balance B

⋮

Old Ledger State

+

Transaction 1

Transaction 2

Transaction 3

Transaction 4

⋮

Transaction Block

=

Account Balance A

Account Balance B

⋮

New Ledger State

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**.

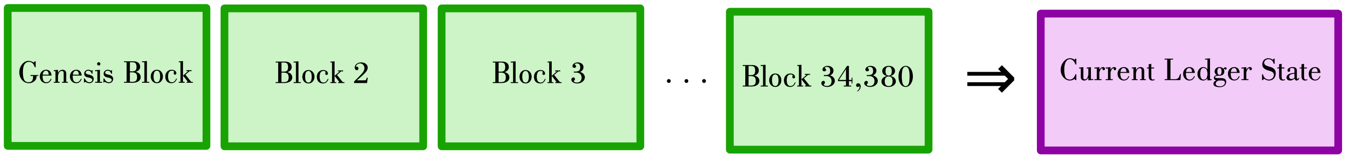
4. Each node checks the current ledger state to see if these transactions are **valid.**

   □ 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.



Genesis Block   Block 2   Block 3 . . . Block 34,380 ⇒ Current Ledger State

The Blockchain

Look! A squirrel!

(Add hand-waving here)

Proof of Work
Proof of Stake
Directed Acyclic Graphs
Mining
Smart Contracts
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 key**s. 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

Problems

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

Cost: It costs about $.75 to make an Ethereum transaction and $3 to make a bitcoin transaction. These have been as high as $4 and $37, respectively. Transactions prices increase when demand for the finite space available in each block goes up.

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 Distributed Ledger Technologies (DLTs) are weak. (Ask me about Byzantine Fault Tolerance)

This Means

□ Bitcoin is not useful as a transactional currency

□ Ethereum is not useful for micropayments

□ It is not clear that Ethereum will be able to support all the ERC20-based startups currently under development once they start writing regular ledger updates into the Ethereum main-chain. Fees will certainly go way up in the next year.

□ It would be neither wise nor practical to move the TSE or any other high value, height transaction volume, entity onto any existing blockchain platform.

Blockchain is Awesome

Having said all that, Blockchain is awesome!

The TSE 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 dis-intermediated.
- □ 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.

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

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.

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 enormous value in a wide array of verticals.

What To Do

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 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.