Blockchain and Crypto Economics: An Example and Deeper Dive

John P. Conley

Vanderbilt University
and
The Geeq Project

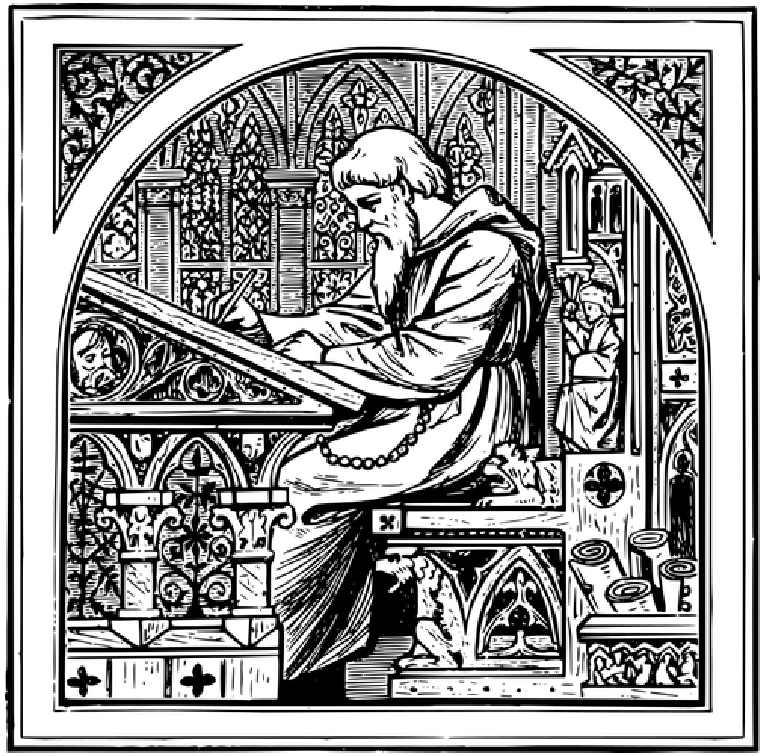
World Bank Mini Boot Camp
Crypto, Information and ICT Economics: What Do We Know?

March 18, 2019

What is Blockchain

What is it?

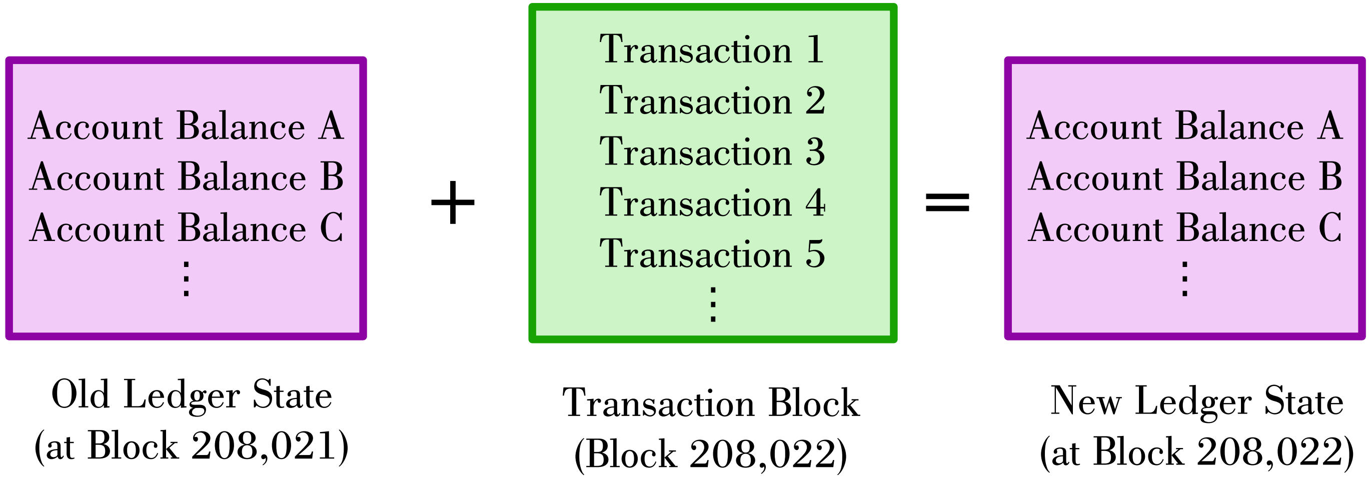
- **Paper ledger books** keep records of account balances, ownership of property, marriages, births, deaths etc.
- Checks or charges made by the account owner were used to **update the balance** held in the account.
- A sale of property would also result in a ledger update.



What is Blockchain?

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?

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

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

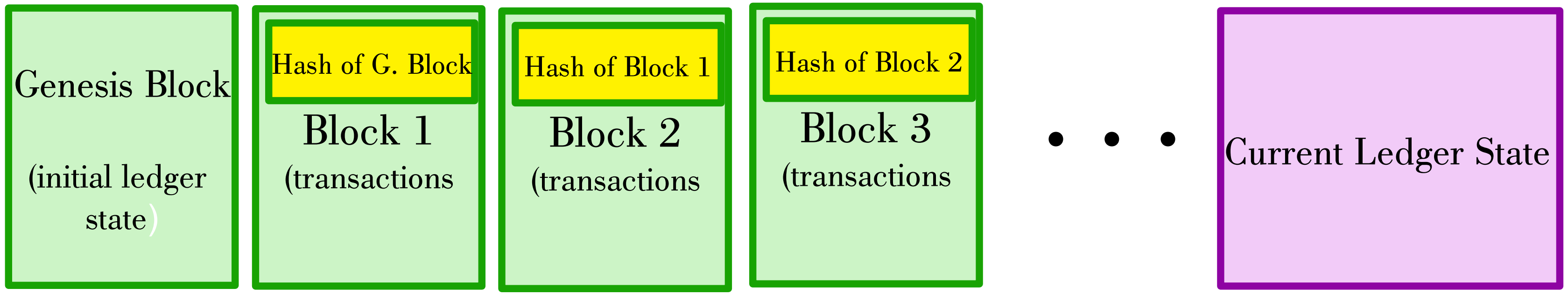
- Each node collects a group of transactions.

- 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?

- 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.

A Blockchain



You might want to have a look at this paper which is a explains the two key technologies that underlie a significant part of ICT:

- Public Private Key (or Asymmetric) Encryption
- Hash Functions

Encryption, Hashing, PPK, and Blockchain: A Simple Introduction

What’s New Here?

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

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

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

What Else is New Here?

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.)

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

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

Important to Understand

Blockchain $\neq$ Bitcoin

Cryptocurrency $\neq$ Cryptotokens

Blockchain $\nRightarrow$ Cryptotokens

Data Systems $\subset$ State Machine Replication Systems $\subset$
Distributed Ledgers $\subset$ 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:

- Allows agents who have never met and do not trust each other to interact and exchange value.
- Does not depend on the good behavior or permission of central authority or data intermediary.
- Provides a credible, immutable, uncensorable source of truth.

Blockchain Use Cases

Payment networks:
Micropayments
Smart cities
Escrows
Internal payment networks

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)

Blockchain and Economics

Macroeconomics

- QTM
- Bubbles
- StableCoins
- Fiscal Policy

Game Theory

- Consensus
- Mechanism Design
- Information and Revelation

Indirectly Related:

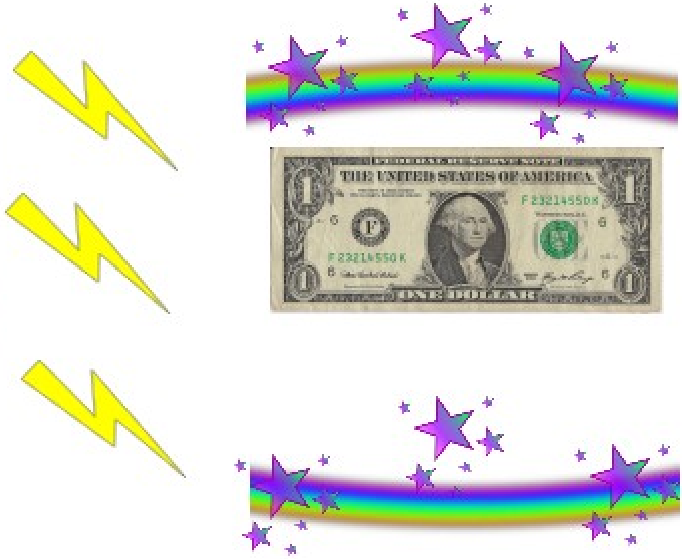
- Finance
- Regulation
- Market Structure
- Behavioral Economics
- Everything Else

Blockchain and Macroeconomics

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

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

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



Blockchain and Macroeconomics

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.

Blockchain and Macroeconomics

We are willing to take 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.

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.

How to Value Cryptocurrencies

Equity Value?: 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. (But ask the SEC about this.)

In most cases when you buy a token, you are not buying a share of the company that issued it. No profits, revenues, or voting power is attached.

By this measure, the value of most cryptotokens should be close to zero.

How to Value Cryptocurrencies

Speculation?: Bitcoin increased in value from $900 to $13,000 from January 2017 to December 2018, and reached a high of $20,000. It is currently valued at about $4,000.

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

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

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

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

How to Value Cryptocurrencies

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 the token (number of times a token is transacted per day).
D = Dollar Value of total transactions per day (PT=D)

The QTM is an accounting identity that says the following:

$$T=MV$$

How to Value Cryptocurrencies

More interestingly:

$$D/P = MV$$

or

$$P = D/MV$$

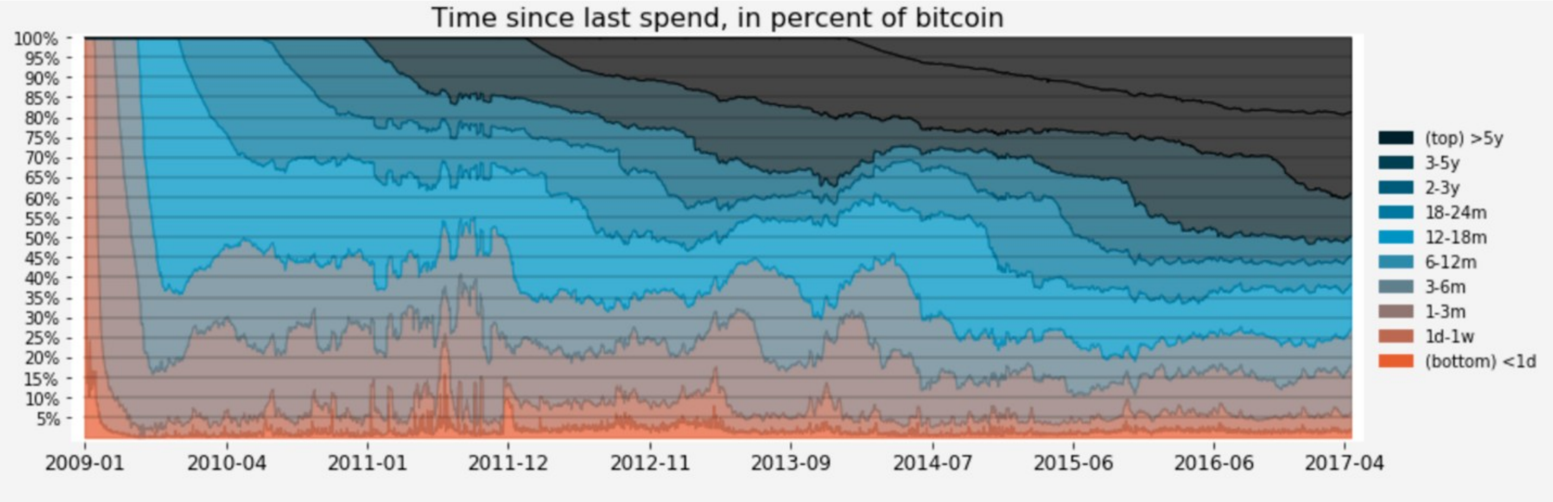
For example, if we need to use 100 goat tokens to buy and sell 800 goats each day and tokens have a velocity of 2, then each token must be worth 4 goats.

How to Value Cryptocurrencies

Which is right? All are right!

- **PV** gives a lower bound on token value.
- **EMT** always holds. The question is, where do expectations come from:
  - FoMO (Fear of Missing Out)
  - Market Manipulation
  - Behavioral Economics
  - Accurate Information?
- **QTM** must hold. In fact you can go to crypto exchanges, calculate daily velocity, see the total quantity of tokens issued and total daily transaction demand, and confirm the price is right.

Old Velocity Data



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

About 20% have not moved in five years, and about half have not moved in the two years. Why?

Stylized Facts

Daily velocities vary between 2 and 6 percent for most actively traded currencies.

Most major concurrency values are highly volatile, but highly correlated.

2108 different tokens listed on coinmarketcap.com, but velocities are close to zero for many almost dead projects.

StableCoins (eg Tether) can have a velocity of 100% or more but have little price volatility

StableCoins are not trustless since they depend of the real banking sector.

Tokencap: Market **$140B** Bitcoin **$71B** Ethereum: **$14B**

Enough Macroeconomics!

Open questions:

- What is a good monetary policy for token creation? (??)
- How can this be credibly committed to? (smart contracts)
- How can you make a trustless StableCoin? (you can’t)
- Can you make a stabilized coin? (you can)
- Can and should KYC/AML be forced onto crypto? (good question)
- Will crypto undermine national fiscal and monetary policy? (maybe)
- What about crypto EFTs, securities, derivatives? (coming)

Game Theory

Blockchains are decentralized ledgers

- This means there has to be agreement on a single state of the ledger (otherwise double spending, etc.).

- Agreement is through **Consensus Games** in which agents called miners, validators, nodes, stakeholders, notaries, etc., vote or use some other mechanism to approve a single new block that all will append to the existing chain.

- All validators are supposed to update the ledger state and keep a copy of all previous blocks they have committed

Consensus Games

- These games arise from a branch of computer science called **Algorithmic Game Theory.**
- Computer scientists think in term of correct and incorrect processes.
- The test is how many of the processes or components can fail and still have the system as a whole work.
- In consensus protocols, nodes are **honest** or **dishonest.**
- **Byzantine Fault Tolerance** (BFT) measures what fraction of dishonest nodes a protocol can have and still produce an honest consensus.

Consensus Games Examples

Proof of Work (PoW): (Bitcoin, Ethereum)

- Miners (30,000 of them) compete to be the first to solve a cryptographic puzzle by brute force. The winner gets to chose the next block and gets a mining reward (and transactions fees).
- Miners waste compute cycles (and electricity) to get this reward: About $25k per block, $2.50 per transaction.
- Longest chain is consider **canonical**.
- Consensus is through the “weight” of effort put into building a chain.
- 50% BFT

Consensus Games Examples

Proof of Stake (PoS): (Tendermint, Algorand, EOS)

- 2/3 stake weighted voting to get canonicalness.
- 33% BFT

Proof of Authority (PoA): (IBM Fabric)

- 2/3 unweighted voting by mutually trusted validators to get canonicalness.
- 33% BFT

BFT and Security

- Two or three mining pools in China own more than half the hashing power of the Bitcoin network.
- It would cost somewhere between $1B and $3B for a bad actor starting from scratch to mount a 51% attack on Bitcoin. Ethereum is even cheaper. Even cheaper if you already have the hardware.
- PoS is even easier to attack. PoA? Don’t ask.
- Who would do such a thing?
  - USA – Stop tax evaders, money launderers, and criminals
  - China or Russia – Cyber warfare.
  - North Korea – Just for fun.
  - Canada?

What Does This All Mean?

- The idea of blockchain is great.

- Blockchain’s potential to change how we interact with one another and how dependent we are central sources of trust and authority is huge.

- No consensus protocol currently in use provides meaningful security

- Plus:
  - Transactions costs are high
  - Scalability is low (few transactions per second)
  - Interoperability is limited.

`

What We Need are Some Economists

- Economists don’t think that anyone is honest. We assume that all agents are self-interested.
- The question to an economist is how to design a game theoretic mechanism that harnesses this self-interest to get the desired outcome.
- Take a mechanism design approach to consensus protocols.
- Implement truth-telling in **coalition-proof equilibrium.**

Problems with Designing a Mechanism

- Multiple equilibria – Proving that there exists a Nash equilibrium in which the validators are honest is meaningless. Games typically have many equilibria, some good, some bad.
- Wrong equilibrium concept – Nash, dominant strategy equilibrium, subgame perfect, sequential, … All are too weak, dependent upon assumptions about information and expectations, and not proof against coordinated actions of coalitions.

Problems with Designing a Mechanism

- Wrong game – A game is a set of players, a strategy space, and payoff functions.
  - Players – Users, ISPs, Sybils, foundations, leaders? Not just nodes.
  - Strategy – Network manipulation, withholding blocks, not following protocols, faking partitions? What actions are available to players?
- Metagame?
  - Nation states may not care about financial payoffs.
  - The value of the information or assets on a blockchain may exceed the cryptocurrency incentives for validators to be honest.

An Example of a Solution

- Proof of Honesty (PoH) – 99% BFT consensus mechanism. PoH works as long as at least one node is honest.
- Catastrophic Dissent Mechanism (CDM) – An audit game/mechanism that implements truth-telling in coalition-proof equilibrium.
- These two mechanisms are part of the protocol driving GeeqChain.

How Does PoH work?

- Any attempt by validators to deviate from Geeq's consensus protocol is immediately and automatically detectable to the user through Geeq's user client.
- Users are able to identify and ignore dishonest validators and refuse to accept transaction/messages on provably dishonest ledgers.
- Users are empowered to protect themselves, which is incentive compatible.
- The BFT requirement that the majority of validating nodes be honest in other protocols builds in an inherent conflict of interest.
- CDM – Ask me later or see the technical paper.

What the Point?

- Any system with self-interested agents, a complicated set of strategies, incomplete information and moral hazard, is a game theory problem
- Blockchain is a game theory problem!
- Solutions can be created to allow anonymous, selfish, colluding agents to facilitate trustless interactions between strangers at low cost.
- You also need to get the computer science, cryptography, information theory, right and then have a sensible business model.
- Even if you do all of the above, you have to get the monetary theory right.
- Finally, you have to actually solve problem (identity, banking the unbanked, etc.)

Other Game Theory in Blockchain

- Governance
- Predictive Markets
- Incentives
- Market Design
- Griefing
- DDoS

Conclusions

- Blockchain is probably the most discussed and least understood technology ever.
- It is the quintessential example of ICT that requires correct design from many fields, economics in particular.
- Information and communication technologies naturally touch on business, finance, and economics so this trend is likely to continue.
- ICT, including blockchain, will almost surely be the major forces driving growth, innovation, and social change in the foreseeable future.
- Economists should take the opportunity to contribute.

Thanks Again!

Links of potential interest:

ETFs Rule, Stablecoins Drool: How to Make Cryptocurrencies go Mainstream

The Economics of Crypto-tokens and Initial Coin Offerings

Encryption, Hashing, PPK, and Blockchain: A Simple Introduction

The Geeq Project:

https://geeq.io/