



Blockchain Technology & Crypto Currency

Alexis Couture



Blockchain Technology: What is it?

Iced Tea Maker's Stock Price Triples After Adding 'Blockchain' to Name [Update]



Bryan Menegus

12/21/17 11:35am • Filed to: BITCOIN



50.5K



69



6



Image: Long Island Iced Tea Corp/Gizmodo

Gizmodo.com

What is a blockchain?

“A blockchain is a data structure that makes it possible to create a **digital ledger** of transactions and share it among a **distributed network** of computers. It uses cryptography to allow each participant on the network to manipulate the ledger in a secure way without the need for a central authority.”

Blockchain at Berkeley – blockchain.berkeley.edu

What are blocks?

- The ledger records transactions in blocks
- Each contains a “cryptographic hash” of the previous block, a timestamp, the transaction date and its own hash.
- A cryptographic hash is information that is converted, through complex algorithms, into a value that can be used to identify/prove the information, but can't be used to recover information.

How is a blockchain built?

1. A transaction occurs.
2. The transaction is verified by the blockchain network – not by a centralized authority – according to rules set by the network
3. The transaction is added to a block and the block is hashed, both with a new hash based on the information contained in the block, and the previous block's hash
4. The block is validated through mathematical work
5. The block is added to the blockchain and distributed to all users in the network

What makes blockchain special?

- No central point of failure/reduction in systemic risk
- Elimination of intermediaries/reduction in operational costs
- Irrevocable and transparent transactions
- (Near) Real-time settlement
- Improved security/fraud minimization

What are the challenges facing blockchain?

- **Transaction speed (only near real time)**
 - This isn't Visa...
- **Energy costs**
 - ING published a paper that a single Bitcoin transaction consumes enough energy to power the “average” household for an entire month – the entire network would consume as much energy as Denmark
- **Recentralization**
- **Lack of regulation (supportive or otherwise)**
 - Can be seen as a positive or a negative
- **Scalability / Interoperability / Standardization**
 - Multiple codes, platforms, uses
- **Market forces**

The types of blockchain

1. Permissionless, public shared systems

- Bitcoin, Ethereum, etc.

2. Federated/consortium blockchains

- Project Jasper – Project involving Payments Canada, the Bank of Canada, TMX Group, Accenture and R3 to evaluate blockchain solutions for the Large Value Transfer System (funds settlement) and CDSX (securities settlement)

3. Permissioned, private shared systems

- Private company systems

Potential uses of blockchain technology

- **Smart contracts**
 - Intersection of law/coding
 - Self-executing, self-enforcing, pre-defined conditions
 - “If this then that”
 - Enforceability?
Jurisdiction? Liability?
Dispute resolution?
- **Digital Identity**
 - Self-sovereign identity (single, secure, portable and immutable identity record not dependent on any centralized authority)
 - Limit access to information, as determined by individual
 - ID2020

Potential uses of blockchain technology

- **Origination / Supply chain**
 - Where something came from and where it has been
 - Title, receipt, authenticity, etc.
 - Internet of things
- **Insurance products**
 - Accelerate claims settlement, reduce fraud and abuse
- **Reward programs**
 - Receive and redeem in real time, reduce fraud and abuse
- **Creation of cryptocurrency**
 - More in a few moments

Popularity of blockchain

- Overhyped? Of 1,053 senior executives in seven countries at companies with more than \$500M in annual revenue, nearly 39% said they believe blockchain is overhyped.
- At the same time, 69% of respondents reported that their organization was spending at least \$1M on blockchain technology in the next calendar year.

Source: Breaking Blockchain Open: Deloitte's 2018 Global Blockchain Survey

Blockchain is not cryptocurrency – but Bitcoin is both



Bitcoin is two things:

1. The protocol/blockchain/ledger (open source code)
2. The coin (code that represents ownership of a digital thing)



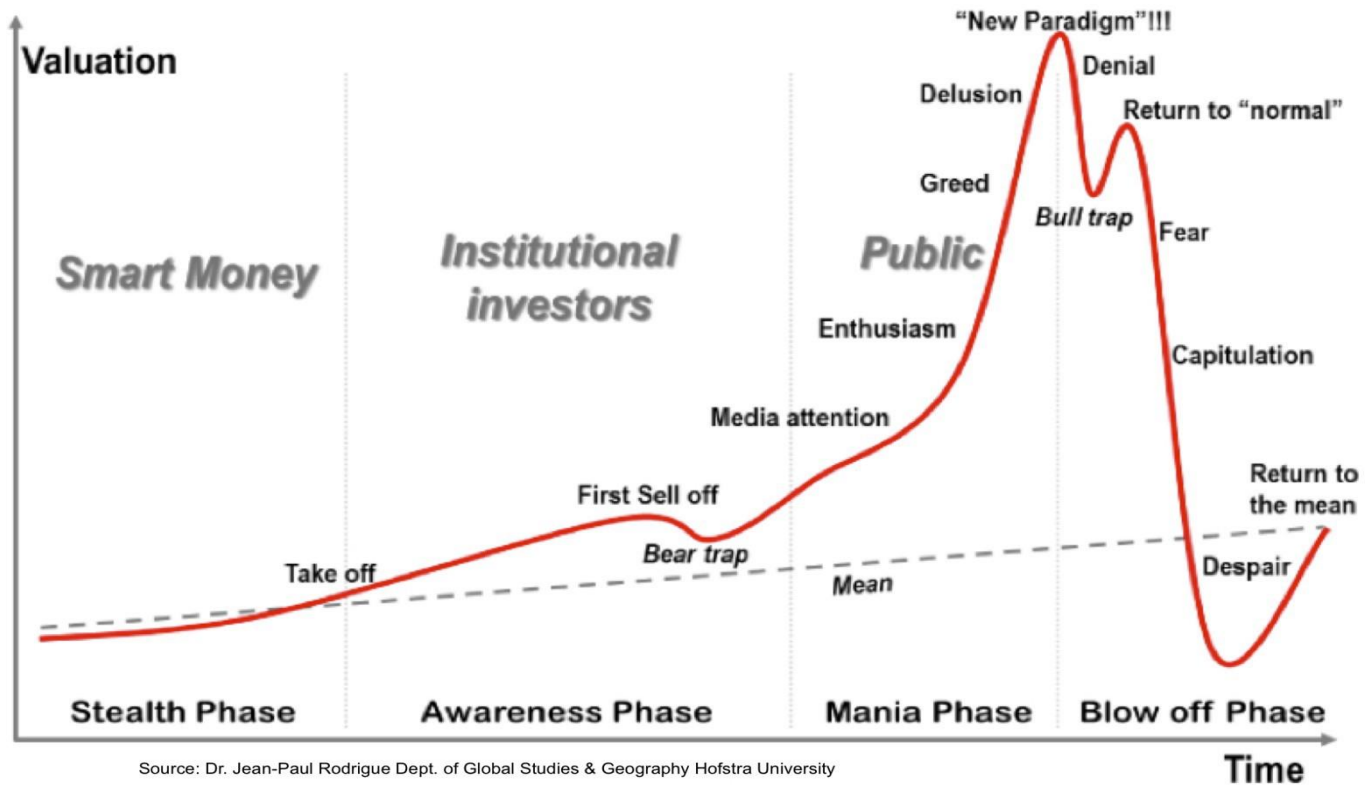
Cryptocurrency:

What is it? What it isn't.

What is cryptocurrency?

- Cryptocurrencies are “things” or “digital assets” built on blockchain technology, but are they:
 - Money?
 - It’s not money per the *Currency Act* because it is not fiat currency.
 - A commodity/good?
 - GST/HST on each transaction? Consumer protection laws.
 - A security / investment contract?
 - The Howey Test
 - Property?
 - Can you take a security interest in Bitcoin?

Value?



Source: Dr. Jean-Paul Rodrigue Dept. of Global Studies & Geography Hofstra University

Price of Bitcoin November 25, 2013 - US\$958.37
Price of Bitcoin December 11, 2017 – US\$17,060.55
Price of Bitcoin April 25, 2019 – US\$5,450.00

MONEY

Man accidentally threw away \$127 million in bitcoin and officials won't allow a search

Published Wed, Dec 20 2017 • 12:30 PM EST • Updated Wed, Dec 20 2017 • 3:24 PM EST



Shawn M. Carter
[@SHAWNCARTER](#)

Share    

Regulations/regulators

- **Securities Commissions** – Regulates securities/capital markets
- **Canada Revenue Agency** – Administers tax laws
- **Bank of Canada** – Regulates monetary policy, the Canadian financial system, currency and funds management
- **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** – Regulates money laundering and the financing of terrorist activities
- **Competition Bureau** – Protects and Promotes competition

The Regulatory Gap



Initial Public Offering (“IPO”) vs. Initial Coin Offering (“ICO”)

- **Process of Sale**
 - IPO: Prospectus, registered dealers, regulated exchange listing
 - ICO: Private transaction, no registered dealers, unregulated exchanges
- **No traditional ownership**
 - IPO: ownership in company/business/issuer, prescribed rights
 - ICO: Digital asset



Why is it important to lawyers?
Practical Implications

How does blockchain impact me?

- **Unique Litigation**
 - Multiple jurisdictions
- **Lawyers as coders?**
 - Where does liability rest? Core developers? Software developers? Miners? Users?
- **Due Diligence**
 - Code, privacy, cybersecurity, etc.

Glossary of terms

Node – User on a blockchain.

Miner – Node who willingly contributes its computing network/resources to store and validate transactions for a fee (usual in the form of the underlying cryptocurrency).

Public Key – A larger numerical value used to encrypt data placed in an open access directory for decryption.

Private Key – Tied to public key, code paired with a public key and used to decrypt and transform a message into readable format.

Token – Cryptocurrency built on top of an existing blockchain. Not native to the particular blockchain. Gives the holder a right to participate in a particular project.

Coin – Digital equivalent of money with similar characteristics: fungible, divisible, acceptable, portable, limited supply. Not intended to perform any function beyond acting as money. Native to the blockchain that created them. e.g. Bitcoin

ICO/ITO – Initial Coin Offering / Initial Token Offering

Hash(ing) – Process of taking an input and turning it into a cryptographic output (a number) through a mathematical algorithm.

Encryption – The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot

Proof of Work – Consensus algorithm to confirm transactions which requires miners to prove they did work to add blocks to the chain. Miners compete to complete transactions on the network (high energy use)

Proof of Stake – Consensus algorithm allocating responsibility of maintaining ledger to those nodes with the largest proposition of virtual currency attached to that blockchain.

Recommended Resources

Blockchain at Berkley

<https://drive.google.com/drive/folders/0B7TsBdkCIBm1c3lzaHBneEt1dU0>

Lisk.io

[Access the power of Blockchain](#)

Canadian Securities Administrators

[CSA Staff Notice 46-307: Cryptocurrency Offerings, 2017](#)

[CSA Staff Notice 46-308: Securities Laws Implications for Offerings of Tokens, 2018](#)

[Consultation Paper 21-402: Proposed Framework for Crypto-Asset Trading Platforms](#)

FINTRAC

[Interpretation Notices and Policy Interpretations](#)

[Compilation of FINTRAC Policy Positions, Outlier Solutions Inc.](#)

Recommended Resources

Canada Revenue Agency

[Guide for Cryptocurrency Users and Tax Professionals](#)
[In-Depth Cryptocurrency Audit Questions](#)

Bank of Canada

[Central Bank Digital Currency: Motivations and Implications](#)

Standing Committee on Banking, Trade and Commerce

[Digital Currency: You Can't Flip this Coin!](#)

University of Cambridge

[Global Cryptocurrency Benchmarking Study, 2017](#)



These materials are intended to provide brief informational summaries of legal developments and topics of general interest.

The materials should not be relied upon as a substitute for consultation with a lawyer with respect to the reader's specific circumstances. Each legal or regulatory situation is different and requires review of the relevant facts and applicable law.

If you have specific questions related to these materials or their application to you, you are encouraged to consult a member of our firm to discuss your need for specific legal advice relating to the particular circumstances of your situation.

Due to the rapidly changing nature of the law, Stewart McKelvey is not responsible for informing you of future legal developments.