Geeking-Out on Crypto

Doug Waggoner

May 3, 2018

ECHO
Transportation Simplified

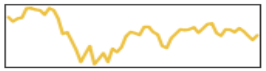
Topics

- Various Coins/Tokens – Ascribing Value
- Mechanics of Coins, Transactions and Mining
- Use Cases for Crypto/Blockchain in Transportation

https://coinmarketcap.com

Top 100 Cryptocurrencies by Market Capitalization

All ▾ | Coins ▾ | Tokens ▾ | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$158,482,998,062	$9,318.61	$8,067,300,000	17,007,150 BTC	0.57%	
2	Ethereum	$68,455,427,776	$690.48	$2,676,650,000	99,141,366 ETH	2.14%	
3	Ripple	$33,416,608,484	$0.853636	$633,135,000	39,146,203,398 XRP *	0.15%	
4	Bitcoin Cash	$24,005,029,298	$1,403.65	$760,271,000	17,101,863 BCH	0.42%	
5	EOS	$15,639,788,588	$18.96	$3,817,280,000	824,939,927 EOS *	-6.91%	
6	Cardano	$9,236,000,338	$0.356230	$348,795,000	25,927,070,538 ADA *	-0.74%	
7	Litecoin	$8,549,716,590	$151.81	$345,448,000	56,318,163 LTC	1.21%	
8	Stellar	$8,171,695,046	$0.440017	$90,052,000	18,571,316,667 XLM *	1.11%	
9	TRON	$6,225,405,975	$0.094686	$1,202,920,000	65,748,111,645 TRX *	12.27%	
10	NEO	$5,729,639,500	$88.15	$612,035,000	65,000,000 NEO *	8.68%	
11	IOTA	$5,550,444,022	$2.00	$68,928,500	2,779,530,283 MIOTA *	0.51%	
12	Monero	$3,907,259,660	$244.46	$83,857,900	15,983,292 XMR	-1.32%	
13	Dash	$3,864,101,512	$480.69	$104,688,000	8,038,673 DASH	-0.36%	

7 Network Effects of Cryptocurrency

- **Speculation** — A cryptographically-backed asset class with the potential for appreciation and high volatility, Bitcoin is perfect for speculators with a high tolerance for risk.
- **Merchant Adoption** — Merchants will increasingly accept Bitcoin because they can increase their profit margins by avoiding credit card fees and chargebacks.
- **Consumer Adoption** — Consumers can use Bitcoin to save money at certain vendors. For example, getting a 20% discount on Amazon by spending Bitcoin through "Purse".
- **Security** — Merchant, consumer, and speculator adoption lead to a higher price and thus incentivize more miners to participate and secure the system. The decentralized, immutable transaction ledger also serves as a form of Triple Entry Bookkeeping, wherein *Debits* plus *Credits* plus the *Network Confirmations* of transactions increase trust and accountability across the system.
- **Developer Mindshare** — Bitcoin is a "dumb", predictable network with simple rules and a publicly-auditable codebase. It is fertile ground for the development of complicated algorithms, machine-to-machine payment protocols, smart contracts, and other tools. Its decentralized nature allows for innovation without permission.
- **Financializing** — Bitcoin will eat up progressively more of the market share of legacy banking institutions in areas such as remittances, micropayments, peer-to-peer lending, and the exchange of stocks and securities.
- **Adoption as a World Reserve Currency** — Potentially, many transactions will be settled on the blockchain, including house titles, stock purchases, car titles, and other monetary instruments and currencies. Network effects one through six culminate in this final network effect.

Bitcoin Wallet – Public Key (Mine)

BTC Wallet Address

3LAyEbDaoTim6o97cigNWxTcvGRW6JxuAy

A Bitcoin Transaction

−0.3300 BTC

≈ $2,973.43

To	1FhHw3hvpQ5k38hycVxXgYtUGtrey6fRwK
Price per coin	$9,010.39
Confirmations	12747
Fee	0.00000000 BTC
Transaction	View transaction

2/1/2018 12:30 PM COMPLETED

ECHO
Transportation Simplified

Bitcoin Transaction Detail

Transaction View information about a bitcoin transaction

c846e5d91f5f540cedd47365b0150ddd6dfabd22e9a894375310b6ef66e7818d

15kTdoGFkjHASqUq9cZxgSZH1H1ixazTEk → 17nBJuAysH2N21WryTmVFM2CAzLTmanSmt 0.985 BTC

12 Confirmations | 0.985 BTC

Summary	
Size	192 (bytes)
Weight	768
Received Time	2018-04-25 16:16:20
Included In Blocks	519886 (2018-04-25 16:17:52 + 2 minutes)
Confirmations	12 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.987 BTC
Total Output	0.985 BTC
Fees	0.002 BTC
Fee per byte	1,041.667 sat/B
Fee per weight unit	260.417 sat/WU
Estimated BTC Transacted	0.985 BTC
Scripts	Show scripts & coinbase

What is Cryptocurrency Mining?

Cryptocurrency mining is a process in which transactions are verified by solving cryptographic problems and then added to the blockchain digital ledger.

Miners use dedicated computer hardware with specialized graphical processing unit (GPU) cards or application-specific integrated circuit (ASIC) chips along with sufficient cooling, an internet connection, mining software package, and membership in an online mining pool.

It's all about a process called "***Hashing***."

Why is Crypto Mined?

- To Facilitate a Decentralized Trustless Ledger
- To Eliminate the Possibility of “Double Spending”
- To Eliminate Tampering and Fraud
- Miners are Rewarded for “Proof of Work”

A Cryptocurrency “Mining Rig”

Cost of this Rig = $4,500

Monthly Profit ~ $500 (paid daily)

Hashing… SHA-256 Algorithm

Input Data

“BAC”

SHA-256 Algorithm

A 256-bit hash is a map from an arbitrary length text message to 256-bit hash value. A 256-bit cryptographic hash is one-way and collision-resistant.

Output (Hash)

313e7c5016db83d1b9741ae1fc33c6e22cc9b36a4935d5371751c39c1862f5a4

(256 bit => 64 hexadecimal Characters)

16^{64} = .1% of the Atoms in the Visible Universe

Hashing – An Example

“Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal. Now we are engaged in a great civil war, testing whether that nation, or any nation so conceived and so dedicated, can long endure. We are met on a great battle-field of that war. We have come to dedicate a portion of that field, as a final resting place for those who here gave their lives that that nation might live. It is altogether fitting and proper that we should do this. But, in a larger sense, we can not dedicate -- we can not consecrate -- we can not hallow -- this ground. The brave men, living and dead, who struggled here, have consecrated it, far above our poor power to add or detract. The world will little note, nor long remember what we say here, but it can never forget what they did here. It is for us the living, rather, to be dedicated here to the unfinished work which they who fought here have thus far so nobly advanced. It is rather for us to be here dedicated to the great task remaining before us -- that from these honored dead we take increased devotion to that cause for which they gave the last full measure of devotion -- that we here highly resolve that these dead shall not have died in vain -- that this nation, under God, shall have a new birth of freedom -- and that government of the people, by the people, for the people, shall not perish from the earth.”

Resultant Hash:

6ACA18EDC5DABF4E7AFA7AA36903AC3731399F23A8236A4518C7B3DB41426F04

Remove the last period and get:

27CF88052BE8DFC1E1DA4C0A8EB09C92140229E27BF43492DFF14219DAE139E3

Hashing as “Proof of Work”

DATA + NONCE => Hash with appropriate difficulty

Northwestern University Transportation Center

Eb69303cf472df08d531f3a8dcc5b89d18aeac3a2936586425c67097c4c0333a

Northwestern University Transportation Center1

d809562812fda8dbe69b7e3e5dbf2a33f7423c84bdbe0f5d772b4cf8a738d696

Northwestern University Transportation Center2

13c267c71fe210da08f157164eb3d4ed2c701570b1be276c4681c96e58dad186

Northwestern University Transportation Center3

54856db8bf8c1edfa35c5303ce255f3e92a0c6c0b2bd2af07c8d7a2e63fafff8

Northwestern University Transportation Center4

e379457f32cc94d96f720213dad6975e2078cf41779f803e51021599c28b71a6

Northwestern University Transportation Center5

004d71c87438f600e2fbd67c6b112a0adcb63447e5273bdb157b299f748f6a4e

A Bitcoin Block

Block Number: 519886

256-bit Hash of the previous block header:
00000000000000003d1372e45a1296f39550172baade06ec5907998f59ed9b

256-bit Hash of all transactions in this block:
4957570818f6b8e6e5f5b1a38cc5e34798dc58e95d88dd17250c873c6f0f1fb7

Time Stamp: 2018-04-25 16:17:52

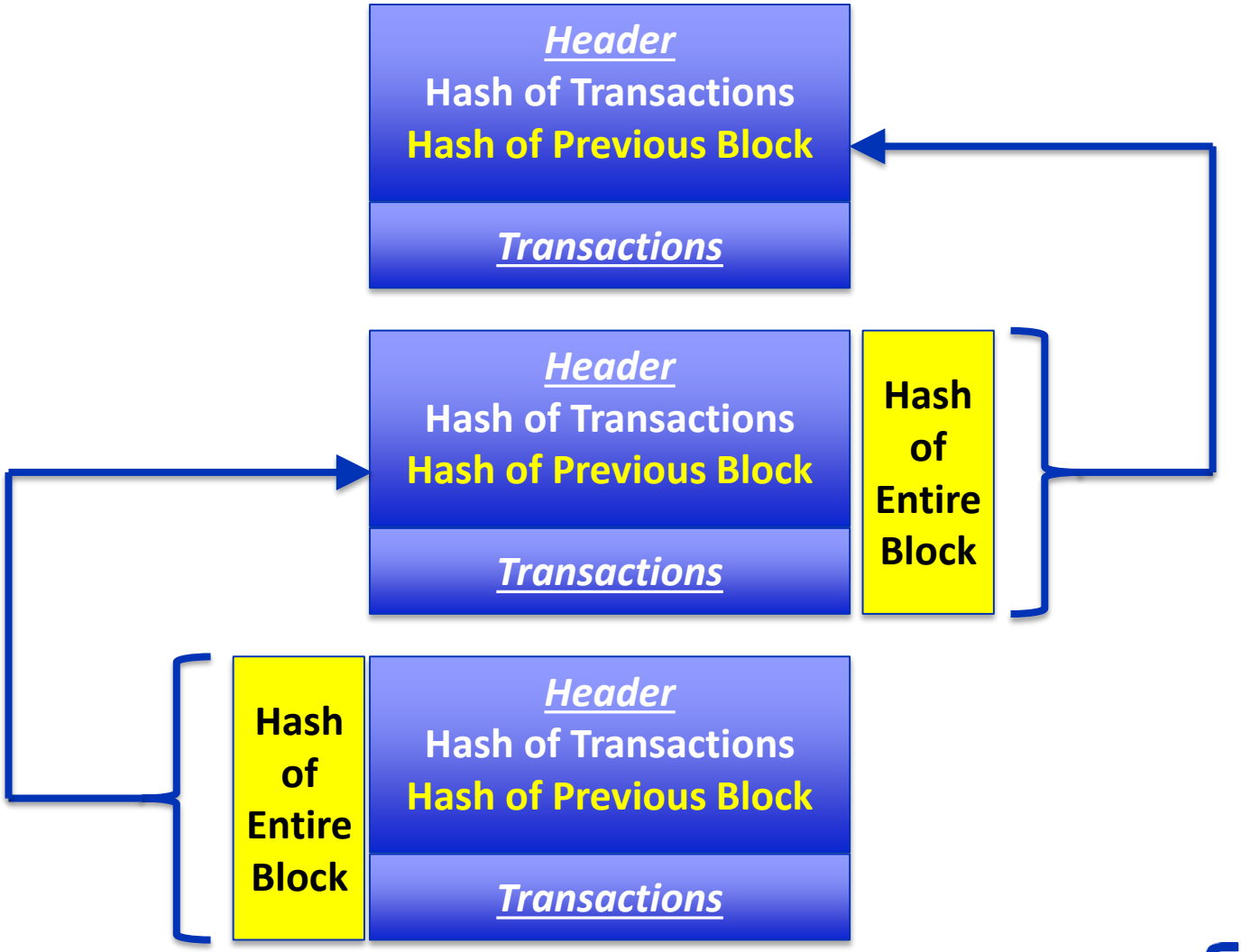
Difficulty Target: 390680589

Nonce: 2205539635

1A2FPavKF4tCUBMRkgaY46bWvABCpYKxWy	158Jzx8fnuHo53G971wwoK9QfvTZxs2GGD	00.9850 BTC
19NxWTS6GSSAug7USHiV48GFqW8JtcL33D	32uZJJf8zLkj4whCiXCKZfmnrKHHd8rFtD	99.9975 BTC
15UqyNk5qTzgdk6SX9juJitzBLkaq6dGSf	15UqyNk5qTzgdk6SX9juJitzBLkaq6dGSf	00.0605 BTC
17x53SrafMtXaCKB5a7awQgYmX1ErWgdKs	1JCPwbCxFzZxwhJ1zNbrpWMSnakgTAss5P	0.00346 BTC
17sWh6rXgGqUM6YALNq4vZ7EPYY36XhUth	1J4thXhzQgTSqrNx5d9cveBcw32bJKQVuw	00.0428 BTC

Hash of this Entire Block (will be included in the Header of the next block):
000000000000000002877cf08bfa152bdf6a1d9681f0590f27e516c6387d6d7

The Immutable Blockchain



ECHO
Transportation Simplified

Use Cases for Transportation

- ***Driver history*** – driver licensing, certifications, safety records, carriers driven for, etc. This history could be securely stored and shared by the driver with potential carrier employers or brokers. Establishing this in widespread use could allow drivers to move between carriers and broker work more seamlessly.

- ***Financial settlement*** – invoicing, critical support documents like BOL and POD documents securely stored and transmitted between shipper, broker, and carrier to establish alignment on payments for all the specific services rendered and proof of those services. Public keys allow for the participants to share information with one another as appropriate (for audit and related reasons). Eventually there could be a high degree of automation to speed payments. Imagine that the truck of a particular delivery has a geo-location device and that there are contract terms based on on-time arrival and/or detention. If the truck is late, the charge from the shipper/consignee could be automated. If the truck arrives on time and is held in the yard because of the warehouse, the charge from the shipper/consignee could be automate, as well.

- ***Supply Chain Transparency and Shipment Tracking*** – secure documentation, geo-location, pallet and container tracking, ship/truck/train status. Putting all these together can digitize critical paperwork, improve status visibility, and share information securely amongst shippers, brokers, consignees, and regulators.

- ***Buying/Selling/Renting optimization algorithms*** – it's possible that companies could plug into a platform or an on-demand TMS Optimization System and access algorithms. Owners of the algorithms will only be willing to do something like this if their intellectual property is protected, which can be afforded via blockchain.

Interesting Crypto Websites

- https://coinmarketcap.com/
- https://blockchain.info/
- https://bitbonkers.com/
- http://passwordsgenerator.net/sha256-hash-generator/
- https://blockchair.com/