The Fundamentals of Bitcoin : How does Bitcoin compare to the competition ?

by Robinson Dorion

JWRD Computing – *Personal Sovereignty through Digital Security*

WoT: dorion, 54CCA1FC8C2E414C63BFB6CF0E48266E54D6B95A

Blog: http://dorion-mode.com
WWW: http://jwrd.net
Email: sales@jwrd.net
Slides :
`http://dorion-mode.com/the-fundamentals-of-bitcoin-20220210.pdf`

February 10, 2022

Overview

1. Bitcoin Protocol

2. Main Competitor Protocol : FED + SWIFT

3. Recap, Questions, Commments

Overview

Bitcoin : Peer to Peer Digital Cash

- Inflation : Mechanism, Enforcement, Verification Costs
- Custody : How is ownership enforced ?
- Transaction Settlement
- Dispute Resolution

Bitcoin Inflation Design

Inflation means money supply growth.

- **Bitcoin is designed for stable, predictable and verifiable money supply growth.**
- Coin supply is incremented approximately every 10 minutes.
- **Hard limit** : there never will be more than 2‘099‘999‘997‘690‘000 satoshis ever in existence (20‘999‘999.97690000 BTC)[1].
- Worth considering : there are currently 46 million millionaires globally.

[1] http://trilema.com/the-sad-state-of-bitcoin-code/#comment-116296

Bitcoin Inflation Mechanism

How do Bitcoin come into existence ?

- A contrived mathematical puzzle : Hashcash Proof of Work.
- A hash[2] function takes an **unbounded input** and produces a **fixed size output**.
- Output is a random, uniform distribution, not known in advance.
- **Mathematical trapdoor function** : inexpensive to compute in one direction, expensive to compute in the opposite direction without special information.
- Guess and check, aka “Mining”.

Bottom Line : resources must be spent to win the new money and change the history of the system, aka “blockchain”.

[2] Hash means to chop up.

SHA 256 Examples

Bitcoin uses Secure Hash Algorithm 256 (SHA256), 256 bit output. 2^{256} is approximately 10^{77}. There are 2 x 10^{23} stars in the universe.

THIS IS SHA256

98b040a3cbb5ae36060729a2b0d57b3c81ae9a1649d4da9b9b554c5478dcf5c2

this is sha256

2f4c6b79b3d0fd07fc30c9dd7aeea0f2b2483801e344eb4253eebb63a2cdc192

Merchant of Venice[3]

48c6489962c0555352ed5d5eafa7962ceea8dbaa9926530fc0fe98d28bc17e92

Bottom Line : slight changes in the input produce substantial changes in the output, varying size inputs produce the same size outputs.

[3] Plaintext from Project Gutenbrg : `https://www.gutenberg.org/ebooks/1515`

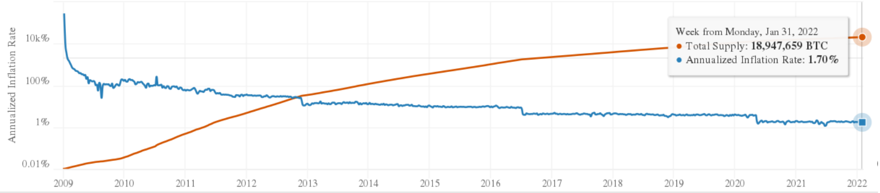
Bitcoin Inflation Control

Challenge : find a SHA256 output with a given number of leading zeros. As competition rises and recedes, the inflation rate stability is maintained by changing the number of leading zeros required to win the reward. Every 210,000 “blocks”, the reward decreases 50%.

Block	Block Hash
Genesis Block :	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Block 1‘337 :	000000008bf44a528a09d203203a6a97c165cf53a92ecc27aed0b49b86a19564
Block 13‘337 :	00000000aeeba6715e296db9b97f0692b58ac77c40199cdb5e4a1116d2059646
Block 133‘337 :	0000000000000608f2af09913562351552e14d10f9250579cc0d89248402be45
Block 210‘000 :	000000000000048b95347e83192f69cf0366076336c639f9b7228e9ba171342e
Block 420‘000 :	000000000000000002cce816c0ab2c5c269cb081896b7dcb34b8422d6b74ffa1
Block 630‘000 :	000000000000000000024bead8df69990852c202db0e0097c1a12ea637d7e96d
Block 721‘915 :	0000000000000000000057c27247655366e08e17b0beb52f9b9245df422083cd

Bottom Line : Difficulty alogorithm adjusts every 2 weeks to maintain a stable inflation rate.

Bitcoin Supply Curve and Annualized Inflation Rate



Takeaway: over 18,925,00 BTC have been mined to date, which is over 90% of the total maximum supply. The annualized inflation rate will remain below 2%.

Bitcoin Inflation Enforcement

How is Bitcoin inflation enforced ?

- Enforced by Network Nodes, Peers.
- Nodes maintain the full transaction history.
- The Protocol is implemented in code. Who you accept software from matters. **Code authors and signers represent counter party risk.**
- "V" is a tool to manage trust.[4]
  - Power Ranger Bitcoin, aka Bitcoin Core, introduced an inflation bug in 2016, was discovered in 2018[5] Informed operators hadn't been accepting their code since 2013[6] or so, bug was never exercised.
  - JWRD Computing maintains[7] reference implementation based on the uncorrupted codebase inherited from Satoshi Nakamoto via Mircea Popescu.

[4] `http://ossasepisa.com/a-walk-among-the-trees-of-v`

[5] `http://qntra.net/power-rangers-inserted-inflation-bug`

[6] `http://dorion-mode.com/the-bitcoin-address-as-a-sign-of-intelligence`

[7] `http://fixpoint.welshcomputing.com/category/bitcoin`

Decentralization Economics

Costs of node maintainance, cost to verify and enforce inflation and receive and broadcast transactions as an independent network peer.

- Intangible Expense
  - Computer literacy, e.g. verifying cryptographic signatures, compiling, installing, configuring software.
  - Scholarship : who has done what deeds and whose words carry weight.
  - Power and Internet Bandwidth.
- Capital Expense
  - Disk
    - 393.3 GB Current Bitcoin Blockchain + Block Index
    - 1 MB / block * 6 blocks / hour * 24 hours / day * 365 days / year = 53 GB / year max growth
    - 1 TB disk can store Bitcoin network at full capacity for over a decade to come
  - RAM : 4 GB recommended
  - CPU : 2 GHz

Bottom Line : intellectual costs are relatively high, capital costs are relatively low.

Bitcoin Custody

He who possesses the key and produces a valid signature has the power to spend.

- Mathematical trapdoor function.
- Bitcoin keys use Elliptic Curve Digital Signature Algorith (ECDSA).[8]
- The private key is the identity.
- **Custody is enforced by operator's ability to keep a 256 bit number secret** and the strength of the mining network.
- Immune to real estate law.

Bottom Line : relatively expensive to steal from an informed operator.

[8] ECDSA public key is hashed with SHA256 (Pay to Pub Key Hash (P2PKH)) and Pub Key Hash is hashed with RIPEMD 160 to produce address.

Bitcoin Transactions

- Miners bundle current transactions waiting for processing with Proof of Work into a “block”.
- **Fungibility :** 1 BTC is 1 BTC, perfectly fungible.
- **Portability :** store locally, broadcast to peers across Internet.
- **Transaction Costs :** Block space is scarce to support network security. Block inclusion prioritized by fee paid per byte.
- **Transaction Time :** 6 block confirmations is standard settlement.
- **Counterparty Risk :** Must be fronted, transactions are irreversible.
    - Best practice for evaluating counterparty risk and establishing identity is RSA key, Web of Trust[9] GPG contracts.[10]
    - Bootstrapped Bitcoin finance, high economic leverage for informed operator.
    - Interest rates established through market process.
    - Intellectually expensive, declined in usage in recent times.

[9] http://trilema.com/what-the-wot-is

[10] http://trilema.com/gpg-contracts

Bitcoin Dispute Resolution

What happens if there's a disagreement on the network ?

Most accumulated proof of work is truth.

Bitcoin Computing Power vs the World

How does Bitcoin rank in terms of computing power globally ?

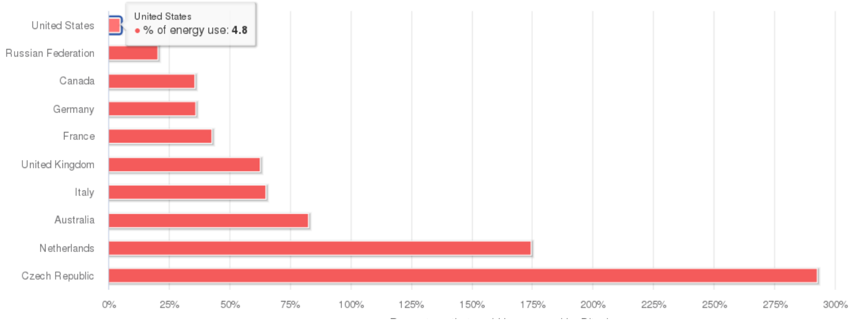
- The Bitcoin network is currently doing approximately 200 Exa hashes per second.
- The Top 500 Supercomputers combined have a maximal performance of 3.04 Exa flops per second.
- 1 hash is approximately 5,000 ALU Flops.
- The Bitcoin network is performing at roughly 1‘000‘000 Exa flops per second, or 1 yotta flop.
- **Concretize :** If the Bitcoin network is the height Trump tower, 284 meters, the top 500 super computers **combined** are 0.9 millimeters tall.

Bottom line : Bitcoin is most powerful phenomenon in human history. Bitcoin isn't just the future, it's the present.

Bitcoin Energy Consumption

Why is Bitcoin's energy consumption a strength ?

Energy consumption is a proxy for the cost to undermine the network.[11]



Bitcoin is consuming more energy to secure the network and money supply than 4 out of every 5 countries on earth.

Bottom Line: The more expensive it is to attack, the more incentive to cooperate.

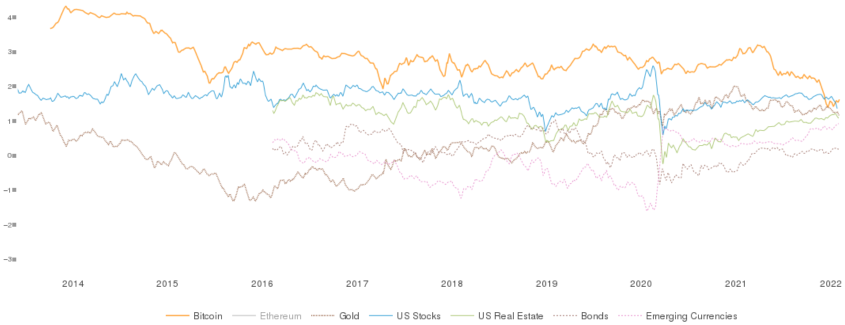
[11] http://trilema.com/the-woes-of-altcoin-or-why-there-is-no-such-thing-as-cryptocurrencies

Bitcoin Phoenix: Bubbles, Crashes, Recoveries

High Date	Price	Low Date	Price	Retrace	Duration
2012/01/12	$7.38	2012/01/27	$3.80	-49%	16 Days
2012/08/17	$16.41	2012/08/19	$7.10	-57%	3 Days
2013/03/06	$49.17	2013/03/07	$33.00	-33%	2 Days
2013/03/21	$76.91	2013/03/23	$50.09	-35%	3 Days
2013/04/10	$259.34	2013/04/12	$45	-83%	3 Days
2013/11/19	$755	2013/11/19	$378	-50%	1 Day
2013/11/30	$1,163	2015/01/14	$152.40	-87%	411 Days
2017/03/10	$1,350	2017/03/25	$891.33	-34%	16 Days
2017/05/25	$2,760.10	2017/05/27	$1850	-33%	3 Days
2017/06/12	$2,980	2017/07/16	$1,830	-39%	35 Days
2017/09/02	$4,979.90	2017/09/15	$2,972.01	-40%	14 Days
2017/11/08	$7,888	2017/11/12	$5,555.55	-30%	5 Days
2017/12/17	$19,666	2018/12/14	$3,230.03	-83%	363 Days
2021/04/14	$64,895	2021/05/23	$31,107	-51%	39 Days
2021/11/09	$68,547	2022/01/22	$35,091	-49%	74 Days

Bottom line : Even buying at bubble tops, with a long term outlook, have yielded real purchasing power gains.

4 year Sharpe Ratio



Bottom Line : On a risk adjusted basis, Bitcoin has outperformed.[12] Bitcoin ranks 15th in global currency market cap.[13]

[12] Source : `http://charts.woobull.com/bitcoin-risk-adjusted-return/`

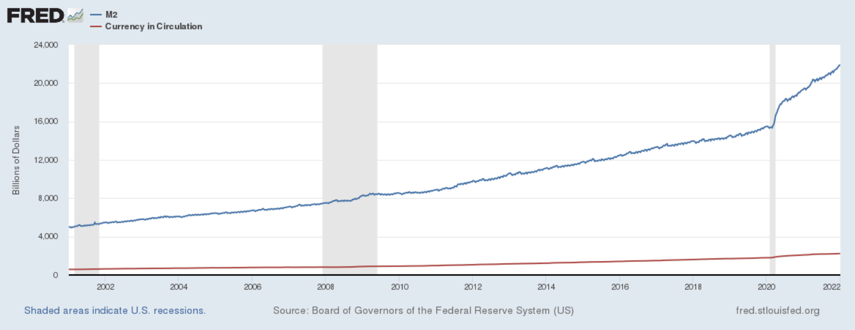
[13] Source : `https://fiatmarketcap.com`

Federal Reserve + SWIFT Inflation Mechanism

- Arbitrary, determined in secret, not independently verifiable.
- Fedspeak, “I would engage in a form of **syntax destruction** which sounded as though I were answering the questions, but, in fact, had not.” - Alan Greenspan, Federal Reserve Chairman 1987-2006
- Inflation information is not independently verifiable. Publication is delayed. Must take Internet website on faith 100%.
- Maximum supply unspecified, in practice, for as long as they can bribe cops with it.
- Can’t raise interest rates or shrink money supply because debt would explode and tax revenue would fall. Thus, kill currency, blame enemies.

Bottom Line : Arbitrary, centrally imposed inflation distorts pricing mechanism and leads to widespread misallocations of capital.

Federal Reserve Inflation



Source: Board of Governors of the Federal Reserve System (US)

Date	FR Note	FR Digital Credit (M2)	M2 Avg Inflation	Cash as % of M2
January 2001	585.1 B	4,984.5 B		11.7%
January 2009	886.2 B	8,329.5 B	8.3%	10.6%
January 2020	1,799.0 B	15,504 B	7.8%	11.6%
January 2022	2,233.7 B	21,844.7 B	20.4%	10.2%

Bottom Line : 90% of Fed Scrip isn't even printed, it's created via certain people appending zeros to the end of their accounts.

Federal Reserve + SWIFT Transaction Mechanism

- Federal Reserve Note
  - Possession is ownership, yet USG property, illegal to destroy.
  - 50% of FRN are held outside USia.
  - $100 maximum note, value melting, more and more cumbersome and risky to transport value.
  - $10,000 border crossing, “civil” asset forefeiture.
- Federal Reserve Digital Credit
  - Correspondents Banks are custodians and operators, they are controlled by/work for the FED.
  - SWIFT system for international transfers. SWIFT is a misnomer.
  - State issued ID number and card, forced to share sensitive information.
  - TLS transaction authentication between client and bank and between banks. Weak, centralized encryption model.
  - Ability to use dependent on political allegiance to whomever won the last US election.
  - Accounts trivially frozen/seized.
  - All transactions over $10k reported as suspicious. Amount was set in 1971, $10k was worth 285 ounces of Gold.
  - Never ending, nor predictible stream of documents to fill. Client must prove innocence regularly.
  - Dispute resolution : for as long as people use, USG will be their judge, jury and executioner.

Bottom Line : Increasingly less useful and fundamentally unsustainable.

Bitcoin vs Fed Scrip

- Identity/Authentication
  - Bitcoin : math based, independently generated and enforced secrets.
  - Fed Scrip : public documents issued by bureaucrats
- Inflation/Money Supply
  - Bitcoin : rooted in math, implemented in open source software, enforced by owners, independently verifiable, stable by design, generated via competition.
  - Fed Scrip : bureaucratic whim
- Interest Rates
  - Bitcoin : established and adjusted via market process.
  - Fed Scrip : bureaucratic whim, artificially suppressed to feed welfare state and buy votes.
- Store of Value
  - Bitcoin : scarce, incentivizing saving and capital accumulation.
  - Fed Scrip : increasingly abundant, incentives spending and capital consumption.

Bitcoin vs Fed Scrip

- Numeraire
  - Bitcoin : able to calculate holdings as percentage of absolute total.
  - Fed Scrip : absolute total unknowable, use as unit of account is a passing fashion.
- Transactions
  - Bitcoin : receive and broadcast independently, perfect fungibility.
  - Fed Scrip : obey increasingly hostile bureaucratic whims or lose access.
- Property Rights
  - Bitcoin : preserves property rights.
  - Fed Scrip : steals and lies as modus operandi.

Bottom Line : That's all.

Questions, Comments

Thank you for your time and attention.

Presentation Slides available for download at:

`http://dorion-mode.com/the-fundamentals-of-bitcoin-20220210.pdf`