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-20230323.pdf`

March 23, 2023

Overview

1. Introduction
2. Fiat was the revolution, Bitcoin is the reaction.
3. Bitcoin Protocol
4. The Protocol in Practice
5. Protocol Risks
6. Being the best Bitcoiner you can be.
7. Parting Quotes, Questions and Comments.

Who am I ?

- From Vermont in Gringolandia.
- Started career as a Private Banker and Investment Consultant with Peter Schiff's Euro Pacific Bank.
- Moved to Panama in January 2013, as I was turning 23.
- In late 2013, realized Bitcoin was superior to "Offshore Banking" and the best instrument for shorting socialist central banking.
- In February 2014, started working in Business Development with Coinapult, a Panama based Bitcoin broker.
- In 2015, formed JWRD Computing with Jacob Welsh.
- JWRD Computing provides Key Management Solutions ranging from hardware, software and operator training.
- Started with minimal to no computer skills. Patience, good teachers and consistent effort have been the keys to success.

Claims to Substantiate

- Due diligence is an essential characteristic of any Bitcoiner worth his salt.
- The satoshi is the world's superlative *numeraire*.
- The Bitcoin network is the biggest computing network on earth, by several orders of magnitude.
- Bitcoin is a substitute for government, a more impactful idea than Aritotle's *Politics*, because it's the strongest system for protecting property rights ever devised.
- Bitcoin is learnable, but *not for everyone*.

Keynes quoting Lenin

The Economic Consequences of the Peace, John Meynard Keynes, 1919

“Lenin is said to have declared that **the best way to destroy the capitalist system is to debauch the currency**. By a continuing process of inflation, governments can confiscate, secretly and unobserved, an important part of the wealth of their citizens...

As the inflation proceeds and the real value of the currency fluctuates wildly from month to month, **all permanent relations between debtors and creditors, which form the ultimate foundation of capitalism, become so utterly disordered as to be almost meaningless**; and the process of wealth-getting degenerates into a gamble and a lottery...

The process engages all the hidden forces of economic law on the side of destruction, and does it in a manner which not one man in a million is able to diagnose.”

Greenspan on the Inflation Tax

Gold and Economic Freedom, Alan Greenspan, published in *The Objectivist* Newsletter, 1966

“The financial policy of the welfare state requires that there be no way for the owners of wealth to protect themselves. This is the shabby secret of the welfare statists’ tirades against gold.

Deficit spending is simply a scheme for the confiscation of wealth.

Gold stands in the way of this insidious process. It stands as a protector of property rights. If one grasps this, one has no difficulty in understanding the statists’ antagonism toward the gold standard.”

Greenspan's Syntax Destruction

60 Minutes, Alan Greenspan with Leslie Stahl.

Leslie Stahl : "That was behind the scenes, in public Greenspan was inscrutible whenever Congress asked about interest rates. He resorted to an indecipherable, Delphic dialect, known as **Fedspeak**."

Alan Greenspan : "I would , I would engage in some form of, uhm, **Syntax Destruction, which sounded as though I were answering the questions, but, in fact, had not.**"

Leslie Stahl : "We showed him a tape of him at a hearing."

Alan Greenspan on tape reading to Congress : "Modest, preemptive actions can obviate the need of more drastic actions at a later date and that could destabilize the economy."

Alan Greenspan : "Very profound."

Leslie Stahl : "Very profound, impenetrably profound. In other words you worked on these."

Alan Greenspan : "Oh, of course !"

Metadata in Bitcoin's Genesis Block

Bitcoin Genesis Block, Satoshi Nakamoto, 2009

> **"The Times 03 Jan 2009 – Chancellor on Brink of Second Bailout for Banks."**

Definitions

Bitcoin : Peer to Peer Digital Cash

- Peer to Peer (P2P) : means there is no trusted third party exercising authority over the history of the system. Peers conduct commerce directly and there is no third party that can stop them if they know what they're doing.
- Digital : rooted in mathematics.
- Etymology of Cash : 1590s, "money box;" also "money in hand, coin," from Middle French *caisse* "money box" (16c.), from Provencall *caissa* or Italian *cassa*, from Latin *capsa* "box".
- **Bitcoin is not trustless**.

Bitcoin Inflation Design

Inflation means an increase in the amount of money in circulation.

- **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].
- Total supply is absolute, current supply is relatively cheap to independently verify.
- **Ownership share and pricing is expressable as a percentage of the total.**
- **The only major currency to decrease the rate of inflation during the panicdemic.**
- 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 reward to 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.
  - Example : Which is harder : "what are the prime factors of 13'843'867 ?" or, "what is the product of 2'029 and 6'823 ?"
- Guess and check by brute force, aka "Mining", is the only known method, which costs resources.

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.

Cryptographic Primitives.

Bitcoin uses Secure Hash Algorithm 256 (SHA256)[3]
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[4]
48c6489962c0555352ed5d5eafa7962ceea8dbaa9926530fc0fe98d28bc17e92

Bottom Line : slight changes in the input produce substantial changes in the output, varying size inputs produce the same size outputs. If you have the input, it's cheap to compute the output ; if you start with an output and want to find its input, it's exceedingly expensive.

[3] The 256 means a bit output.

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

Bitcoin Inflation Control

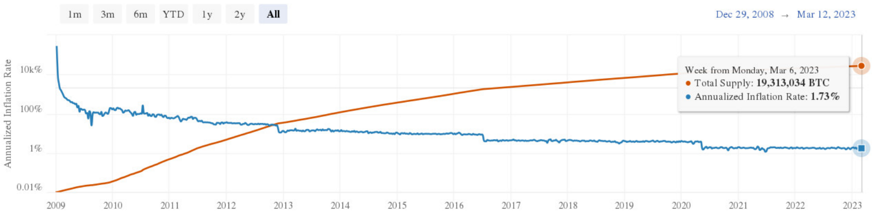
Challenge : find a SHA256 output with a given number of leading zeros. As competition rises and recedes, the inflation rate stability is maintained by changing the number of leading zeros required to win the reward.

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
Block 780‘707 :	0000000000000000000412921015c683dc5480076a2d91e60a4513bd9fe7a55e

Bottom Line : Difficulty alogorithm adjusts every 2 weeks to maintain a stable inflation rate and allows the system to adapt to market forces.

Bitcoin Supply Curve and Annualized Inflation Rate

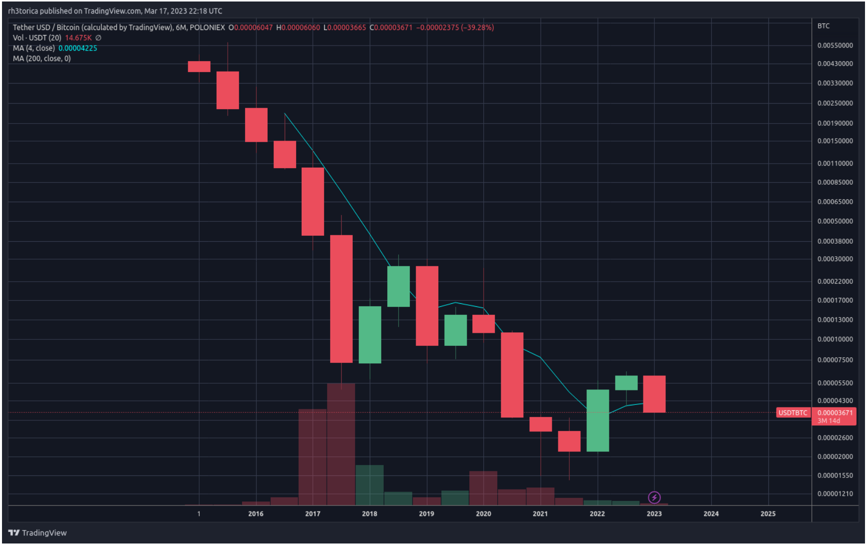
Every 210,000 “blocks”, the reward decreases 50%.



Week from Monday, Mar 6, 2023
● Total Supply: **19,313,034 BTC**
● Annualized Inflation Rate: **1.73%**

Takeaway: over 19,313,000 BTC have been mined to date, which is over 92% of the total possible supply. The annualized inflation rate will remain below 2%.

The Dollar measured in Satoshi



Takeaway: The purchasing power of one Dollar has declined from 444‘444 satoshi on Jan 1, 2015 to 3‘658 satoshi currently.

A loss of over 99%.

Bitcoin Inflation Enforcement

How is Bitcoin inflation enforced ?

- Enforced by network *nodes*, run by people called *Peers*.
- Nodes are computers running the Bitcoin software which verify and 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.[5]
  - Power Ranger Bitcoin, aka Bitcoin’s rotten core, introduced an inflation bug in 2016, was discovered in 2018.[6] Informed operators hadn’t been accepting their code since 2013[7] or so, bug was never exercised.
  - JWRD Computing maintains[8] the Bitcoin reference implementation based on Satoshi Nakamoto’s final release. *The most conservative implementation of Bitcoin.*
- No one has any claim to title in law or equity of yet-unmined Bitcoin. Bitcoin is immune to real estate law. In Bitcoin, there is a positive incentive to mine.

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

[6] https://archive.is/3Uyyn

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

[8] http://fixpoint.welshcomputing.com/category/bitcoin

Decentralization Economics : The Cost of Peerage

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

- Tangible Capital Costs
  - Disk
    - 440 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 about a decade to come
  - RAM : 4 GB recommended
  - CPU : 2 GHz
- Intangible Costs
  - Power and Internet Bandwidth.
- Intellectual Costs
  - Computer literacy, e.g. verifying cryptographic signatures, compiling, installing, configuring software. Best learned via Command Line Interface[9]
  - Scholarship : who has done what deeds and whose words carry weight.

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

[9] http://dorion-mode.com/2021/12/open-you-blind-eyes-with-cli-literacy/

Bitcoin Custody

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

- Bitcoin is an alodial title system[10], which means it's property in the proper sense, i.e. can actually be owned by its owner and not subordinated to any higher-ranking proprietor.
- The private key is the identity according to the protocol.
- Custody is protected by *mathematical trapdoor functions* and the mining network.
- Bitcoin keys use Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA key is hashed twice using SHA256 and then hashed using RIPEMD 160 to establish the *address*.
- **Custody is enforced by operator's ability to keep a 256 bit number secret** and the strength of the mining network.

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

[10] http://fixpoint.welshcomputing.com/2021/lets-learn-words/

Bitcoin Private Key and Public Address

Private Key:

6b2c 0335 3c50 f50b
d9ed da0a 9856 a89d
911b 8c7a 5289 fa3f
10f5 b47d a2c6 d5a7

Public Address:

1DtQXKanLPFYBszPPTGToA6YWnxeeiowQM

How small could you write such a number ? How well could you hide it among the thousands of other digital files you carry around ?

Bitcoin Transactions

- Miners bundle current transactions signed 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.
- **No Consideration :** All purchases of Bitcoin are contracts for no consideration and legally without merit.[11]
- **Counterparty Risk :** Must be fronted, transactions are irreversible.
  - Best practice for evaluating counterparty risk and establishing identity is RSA key, Web of Trust[12] GPG contracts.[13]
  - Bootstrapped Bitcoin finance, high economic leverage for informed operator.
  - Interest rates established through market process.
  - Intellectually expensive, declined in usage in recent times.

[11] http://trilema.com/the-reasons-why-bitcoin-securities

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

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

Bitcoin Dispute Resolution

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

The 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 357.71 Exa hashes per second.[14]
- The Top 500 Supercomputers combined have a maximal performance of 4.86 Exa flops per second.[15]
- 1 hash is approximately 5,000 ALU Flops.
- The Bitcoin network is performing at roughly 1‘788‘550 Exa flops per second, or 1.79 yotta flop.
- **Concretize :** If the Bitcoin network is the height Torre Towerbank (231 meters) the top 500 super computers **combined** are 0.627 millimeters tall.

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

[14] Terra, Peta, Exa, Zetta, Yotta

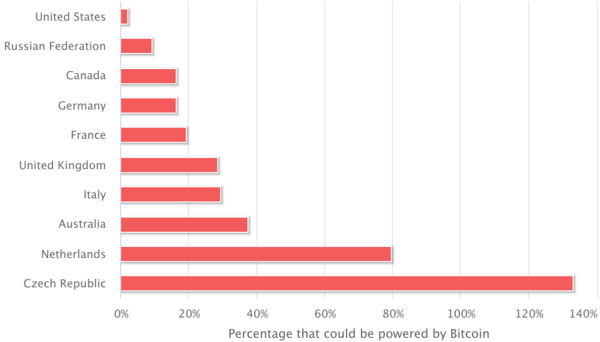
[15] https://top500.org/lists/top500/2022/11/

Bitcoin Energy Consumption

Why is Bitcoin's energy consumption a strength ?

Energy consumption is a proxy for the cost to undermine the network.[16]

Bitcoin Energy Consumption Relative to Several Countries



BitcoinEnergyConsumption.com

Bitcoin ranks 35th in energy consumption and 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.

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

Protocol Risks Part 1

"You know what gets no airplay ? The unflattering truth."

- The protocol is not specified. The rotten core has piled on complexity as opposed to cleaning up the code Satoshi left.
- Compromise of cryptographic primitives.
- Nodes provide a valuable service, but are not renumerated and costs continually increase. Miners aren't required to run full nodes. This undermines decentralization.[17]
- Targeted censorship by miners of valid transactions, example BitBet 2016.[18]
- Asymptotes don't exist in nature, at some point a phase transition will occur and it will make more sense for miners to start a new Bitcoin.
- Social Engineering is the #1 ongoing threat to individuals and organizations.

[17] http://trilema.com/2016/the-necessary-prerequisite-for-any-change-to-the-bitcoin-protocol/

[18] `https://archive.is/JazT0`

Protocol Risks Part 2

"There is nothing new in the world apart from the history you didn't know."

- Hardfork : a change in the protocol that accepts blocks which were not previously valid, requires economic consensus to succeed. Example : Bitcoin Cash.
- Softfork : a tightening of the rules that censors transactions that are valid. Does not require economic consensus to prevail in the short run, the long run is a different story though.
  - Dangerous examples : "Multi-sig" and "Segregated Witness", both of which weaken the key security for the users.[19] As described by their author's, they are "ANYONE CAN SPEND" coins.
  - Softfork risk mitigation #1 : exclusively use valid Bitcoin addresses, Pay to Public Key Hash (P2PKH), which all start with the number "1".
  - Softfork risk mitigation #2 : exclusively run node software that predates version 0.6.

Bottom line : Evolution is a slow and sloppy process. As long as Bitcoin survives it will continue to wage a war of attrition against socialism. Bitcoin is a refuge for the elites defecting from the bankrupt socialist regime.

Alea iacta est.

[19] http://dorion-mode.com/2021/the-bitcoin-address-as-a-sign-of-intelligence

The Evolution of a Bitcoiner Part 1

Understand you come from a socialist environment and have to unlearn many things.

- Holy due diligence :
  - Who has credibility ? Who was saying what and when ? Who was warning about scams and who was sinking them ?
  - Who holds economic weight ?
  - Whose words and actions indicate commitment to making Bitcoin the best it can be ?
  - Who wants to make Bitcoin more like fiat ?
  - The Superlative Entrypoint : Trilema's Bitcoin category `http://trilema.com/category/bitcoin`
- Curate your mind and a network :
  - Lesson your dependency on Silly Con Valley technology and information streams, "the medium is the message."
  - Establish trading relationships and build trust with individuals.
  - Refuse to send to anything other than addresses starting with "1".
  - Don't forget to laugh and have fun as you grow !

"Your worst enemy has always slept in the same bed as you."[20]

[20] http://ossasepia.com/2022/06/23/all-tattoos-are-temporary/

The Evolution of a Bitcoiner Part 2

"Hard work pays off in the future. Laziness pays off now."[21]

- Key management :
  - Use hardware that is not backdoored.
  - Use a cryptographic entropy source for your private keys.
  - Learn to use an open source operating system.
  - Improve your computer literacy, e.g. compiling source code, configuring firewalls.
  - Exclusively use Bitcoin addresses which start with "1".
  - Leverage strong tools for encryption, e.g. RSA.
  - Run a Bitcoin node which doesn't recognize the dangerous softforks, i.e. pre version 0.6.
  - Mind your step.

Bottom line : Bitcoin is for the few, not the many.
Which are you ?

"The strongest indication that you lost your way is to find a large majority in agreement with you."[22]

[21] http://ossasepia.com/2022/06/23/all-tattoos-are-temporary/

[22] http://ossasepia.com/2022/06/23/all-tattoos-are-temporary/

Keynes on Intellectual Slavery

The General Theory of Employment, Interest and Money, John Meynard Keynes, 1936

"The ideas of economists and political philosophers, both when they are right and when they are wrong, are more powerful than is commonly understood. Indeed the world is ruled by little else. **Practical men who believe themselves to be quite exempt from any intellectual influence are usually the slaves of some defunct economist.**"

Popescu on Intellectual Manumission

A conceit, or the importance of blogging.[23]
Mircea Popescu, 2014

"So my friends : do not be afraid of all the things that are scary. The most they can do while under your gaze is make you stronger. **Be instead afraid of the things you make no effort to understand, because from behind they can give you quite the sound trashing.** And the worst part of it is... you'll likely never know."

[23] `http://trilema.com/2014/a-conceit-or-the-importance-of-blogging/`

Questions, Comments

Thank you for your time and attention.

Presentation Slides available for download at:

`http://dorion-mode.com/the-fundamentals-of-bitcoin-20230323.pdf`